Guernsey Financial Services Commission

Handbook on Countering Financial Crime (AML/CFT/CPF)

5 May 2026

Contents

Chapters of this Handbook

Table of Acronyms

The following acronyms are used within this *Handbook*. Where necessary definitions of these terms can be found in Appendix A.

AI	Artificial Intelligence
AML	Anti-Money Laundering
App	Application
BACS	Bankers' Automated Clearing System
CDD	Customer Due Diligence
CECIS	Closed-Ended Collective Investment Scheme
CFT	Countering the Financing of Terrorism
CMP	Compliance Monitoring Programme
CPF	Countering the Financing of Proliferation of Weapons of Mass Destruction
CIS	Collective Investment Scheme
DT	Drug Trafficking
ECDD	Enhanced Customer Due Diligence
ESAs	European Supervisory Authorities
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSB	Financial Services Business
GP	General Partner
IBAN	International Bank Account Number
IC	Incorporated Cell
ICC	Incorporated Cell Company
IFSWF	International Forum of Sovereign Wealth Funds
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
IT	Information Technology
LCF	Lending, Credit and Finance
LLP	Limited Liability Partnership
LP	Limited Partnership
LPP	Legal Professional Privilege
MI	Management Information
ML	Money Laundering
MLCO	Money Laundering Compliance Officer
MLRO	Money Laundering Reporting Officer
MONEYVAL	The Committee of Experts on the Evaluation of Anti-Money Laundering and the Financing of Terrorism
MSP	Money Service Provider
MVTS	Money or Value Transfer Service
NATO	North Atlantic Treaty Organization
NGCIS	Non-Guernsey Collective Investment Scheme
NPO	Non-Profit Organisation
NRA	National Risk Assessment
OECD	Organisation for Economic Co-operation and Development

OECIS	Open-Ended Collective Investment Scheme
OFAC	Office of Foreign Assets Control
PB	Prescribed Business
PC	Protected Cell
PCC	Protected Cell Company
PEP	Politically Exposed Person
PF	Proliferation Financing
PQ	Personal Questionnaire
PSP	Payment Service Provider
RFID	Radio-Frequency Identification
SCDD	Simplified Customer Due Diligence
SDN	Specially Designated National
SIO	Senior Investigating Officer
SWF	Sovereign Wealth Fund
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TCSP	Trust and Corporate Service Provider
TF	Terrorist Financing
THEMIS	The FIU Online Reporting Facility for a Disclosure of Suspicion
UK	United Kingdom
UN	United Nations
UNSCR	United Nations Security Council Resolutions
US	United States of America
VA	Virtual Asset
VASP	Virtual Asset Service Provider
WMD	Weapons of Mass Destruction

Table of Figures

The following tables and diagrams are used within this *Handbook*:

Chapter 1
Introduction

Contents of this Chapter

1.1. Introduction

1. The laundering of criminal *proceeds*, the financing of terrorism and proliferation financing (henceforth referred to collectively as "ML, TF and PF") through the financial and business systems of the world is vital to the success of criminal, terrorist and proliferation operations. To this end, criminals, terrorists and proliferators seek to exploit the facilities of the world's businesses in order to benefit from such *proceeds* or financing.

2. Increased use of technology and integration of the world's financial systems, combined with the removal of barriers to the free movement of capital, have enhanced the ease with which criminal *proceeds* can be laundered or terrorist or proliferation funds transferred and have added to the complexity of audit trails. The future of the Bailiwick of Guernsey ("*the Bailiwick*") as a well-respected international financial centre depends on its ability to prevent the abuse of its financial services business ("*FSB*") and prescribed business ("*PB*") sectors by criminals and terrorists.

1.2. Background and Scope

3. *The Bailiwick* authorities are committed to ensuring that criminals, including money launderers, terrorists and those financing terrorism or the proliferation of weapons of mass destruction, cannot launder the *proceeds* of crime through *the Bailiwick* or otherwise use *the Bailiwick's* finance and business sectors. The Guernsey Financial Services Commission ("*the Commission*") endorses the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation issued by the Financial Action Task Force ("FATF" and "*the FATF Recommendations*"). This *Handbook* is a statement of the standards expected by *the Commission* of all *specified businesses* in *the Bailiwick* to ensure *the Bailiwick's* compliance with *the FATF Recommendations*.

4. Should a *specified business* assist in *ML*, *TF* and/or *PF*, it could face regulatory investigation, the loss of its reputation, and law enforcement investigation. The involvement of a *specified business* with criminal *proceeds*, terrorist funds or proliferation financing would also damage the reputation and integrity of *the Bailiwick* as an international finance centre.

5. Throughout this *Handbook* references to *PF* relate solely to the breach, non-implementation, circumvention or evasion of targeted financial sanctions that are imposed under any international sanctions measure implemented in *the Bailiwick* which relate to the proliferation of weapons of mass destruction ("WMD") and its financing. The term "proliferator" is used in the Handbook to refer to those involved in *PF* which could include State actors seeking to enhance their own WMD, individuals or entities seeking to profit from proliferation of WMD and terrorist groups which may acquire or develop WMD for use in terrorist acts. References to WMD relate to biological, chemical or nuclear (including radiological) weapons.

6. Under Section 1(1) of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended ("*the Law*") all offences that are indictable under the laws of *the Bailiwick* are considered to be predicate offences and therefore funds or any type of property, regardless of value, acquired either directly or indirectly as the result of committing a predicate offence, are considered to be the *proceeds* of crime. Under *Bailiwick* law all offences are indictable, with the exception of some minor offences which mainly concern public order and road traffic. The range of predicate offences is therefore extremely wide and includes, but is not limited to, the following:

   (a) participation in an organised criminal group and racketeering;
   (b) terrorism, including *TF*;
   (c) financing of proliferation of weapons of mass destruction;
   (d) human trafficking and migrant smuggling;
   (e) sexual exploitation, including sexual exploitation of children;

(f) illicit trafficking in narcotic drugs and psychotropic substances;
(g) illicit arms trafficking;
(h) illicit trafficking in stolen and other goods;
(i) corruption and bribery;
(j) fraud and tax evasion;
(k) counterfeiting and piracy of products;
(l) environmental crime;
(m) murder, manslaughter and grievous bodily injury;
(n) kidnapping, illegal restraint and hostage taking;
(o) robbery and theft;
(p) smuggling;
(q) extortion;
(r) forgery;
(s) piracy; and
(t) insider trading and market manipulation.

7. *The Bailiwick's* anti-money laundering ("AML"), countering the financing of terrorism ("CFT") and countering the financing of proliferation of weapons of mass destruction ("CPF") legislation (and by extension this *Handbook*) applies to all *specified businesses* conducting business in *the Bailiwick*. This includes *Bailiwick*-based branches and offices of companies incorporated outside of *the Bailiwick* conducting financial services and/or prescribed business within *the Bailiwick*. In this *Handbook* all references to 'the firm' shall have the same meaning as *specified business* in Paragraph 21(1) of *Schedule 3*, and includes all such businesses whether natural persons, *legal persons* or *legal arrangements*, including but not limited to, companies, partnerships and sole traders.

8. *Schedule 3* to *the Law* (referred to henceforth as "*Schedule 3*") and this *Handbook* have been drafted to take into account the fact that not all of the requirements of *the FATF Recommendations* are relevant to all businesses. In this regard, while certain provisions (for example, the application of a *risk*-based approach, corporate governance, *customer due diligence* ("*CDD*"), suspicion reporting, *employee* training and record keeping) apply equally to all firms, there are other requirements set out in this *Handbook* which may not be as relevant to some particular areas of industry (for example, *wire transfers* and *virtual assets*). Taking such an approach to the drafting of *Schedule 3* and this *Handbook* is intended to prevent the application of unnecessary and bureaucratic standards.

1.3. The Bailiwick's AML, CFT and CPF Framework

9. *The Bailiwick's* AML, CFT and CPF framework includes the following legislation (henceforth referred to as "*the Relevant Enactments*"):

(a) The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999;
(b) The Drug Trafficking (Bailiwick of Guernsey) Law, 2000;
(c) The Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011;
(d) The Sanctions (Bailiwick of Guernsey) Law, 2018;
(e) The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002;
(f) The Disclosure (Bailiwick of Guernsey) Law, 2007;
(g) The Transfer of Funds (Guernsey) Ordinance, 2017;
(h) The Transfer of Funds (Alderney) Ordinance, 2017;
(i) The Transfer of Funds (Sark) Ordinance, 2017;
(j) The Disclosure (Bailiwick of Guernsey) Regulations, 2007;
(k) The Terrorism and Crime (Bailiwick of Guernsey) Regulations, 2007;
(l) The Prescribed Businesses (Bailiwick of Guernsey) Law, 2008;
(m) The Beneficial Ownership of Legal Persons (Guernsey) Law, 2017;
(n) The Beneficial Ownership of Legal Persons (Alderney) Law, 2017;

(o) The Beneficial Ownership (Definition) Regulations, 2017;
(p) The Beneficial Ownership (Alderney) (Definitions) Regulations, 2017;
(q) The Beneficial Ownership of Legal Persons (Provision of Information) (Transitional Provisions) Regulations, 2017;
(r) The Beneficial Ownership of Legal Persons (Provision of Information) (Transitional Provisions) (Alderney) Regulations, 2017;
(s) The Beneficial Ownership of Legal Persons (Nominee Relationships) Regulations, 2017;
(t) The Beneficial Ownership of Legal Persons (Nominee Relationships) (Alderney) Ordinance, 2017; and
(u) The Beneficial Ownership of Legal Persons (Provision of Information) (Limited Partnerships) Regulations, 2017;

and such other enactments relating to *ML, FT* and *PF* as may be enacted from time to time in *the Bailiwick.*

10. Sanctions legislation is published by the States of Guernsey's Policy & Resources Committee and can be accessed via the below website:

www.gov.gg/sanctions

1.4. Handbook Purpose

11. This *Handbook* has been issued by *the Commission* and, together with statements and instructions issued by *the Commission*, contains the rules and guidance referred to in: Sections 49AA(7) and 48MB(1)of *the Law*; Paragraph 3(7) of *Schedule 3* to *the Law*; Sections 15(8) and 74C(1) of the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 as amended ("*the Terrorism Law*"); Section 15 of the Disclosure (Bailiwick of Guernsey) Law, 2007 as amended ("*the Disclosure Law*"); and Section 11 of the Transfer of Funds (Guernsey) Ordinance, 2017, the Transfer of Funds (Alderney) Ordinance, 2017 and the Transfer of Funds (Sark) Ordinance, 2017 ("*the Transfer of Funds Ordinance*").

12. This *Handbook* is issued to assist the firm in complying with the requirements of the relevant legislation concerning *ML, TF* and *PF* financial crime and related offences to prevent *the Bailiwick's* financial system and operations from being abused for *ML, TF* and *PF*. *The Law* and *the Terrorism Law* as amended state that *the Bailiwick* courts shall take account of rules made and instructions and guidance given by *the Commission* in determining whether or not the firm has complied with the requirements of *Schedule 3*.

13. This *Handbook* has the following additional purposes:

(a) to outline the legal and regulatory framework for AML, CFT and CPF requirements and systems;
(b) to interpret the requirements of *the Relevant Enactments* and provide guidance on how they may be implemented in practice;
(c) to indicate good industry practice in AML, CFT and CPF procedures through a proportionate, *risk*-based approach; and
(d) to assist in the design and implementation of systems and controls necessary to mitigate the *risks* of the firm being used in connection with *ML, TF* and *PF* and other financial crime.

14. The *Commission* acknowledges the differing approaches adopted by *specified businesses* to achieve compliance with the requirements of *the Relevant Enactments* and *Commission Rules*. The Commission encourages all firms to consider how developments in technology could assist them in complying with their obligations as well as streamlining business processes. This *Handbook* therefore seeks to adopt a technology positive stance, allowing firms to embrace

whichever technological solution(s) they have assessed and deem appropriate to meet their obligations. The Handbook still allows firms to utilise existing measures to meet their obligations, provided those measures remain effective, proportionate and do not unduly prevent other firms' use of technology, for example, by refusing to accept a signature in electronic form or electronically certified/verified *CDD* documentation as allowed by this *Handbook*. Further information about the use of technology can be found in Chapter 3 of this *Handbook*.

1.5. Requirements of Schedule 3

15. *Schedule 3* includes requirements relating to:

(a) *risk* assessment and mitigation;
(b) applying *CDD* measures;
(c) monitoring *customer* activity and ongoing *CDD*;
(d) reporting suspected *ML*, *TF* and *PF* activity;
(e) *employee* screening and training;
(f) record keeping; and
(g) ensuring compliance, corporate responsibility and related requirements.

16. Any paraphrasing of *Schedule 3* within parts of this *Handbook* represents *the Commission's* own explanation of that schedule and is for the purposes of information and assistance only. *Schedule 3* remains the definitive text for the firm's AML, CFT and CPF obligations. *The Commission's* paraphrasing does not detract from the legal effect of *Schedule 3* or from its enforceability by the courts. In case of doubt, you are advised to consult a *Bailiwick* Advocate.

17. In addition to the requirements of *Schedule 3*, section 48MA of *the Law* and section 74A of *The Terrorism Law* include offences relating respectively to failure to prevent money laundering and failure to prevent terrorist financing. Under these sections a firm licensed under *the Regulatory Laws* (for the purposes of this section, the "licensed firm") is guilty of an offence if a person is engaged in money laundering or terrorist financing when acting in the capacity of a person associated with the licensed firm, unless the licensed firm can prove it had in place prevention procedures in relation to the activities of the person associated with the licensed firm when the money laundering or terrorist financing offence occurred.

18. If the licensed firm has in place effective policies, procedures and controls to counter *ML*, *TF* and *PF* which are in line with the requirements of *Schedule 3* and the *Handbook*, they could be considered towards prevention procedures in relation to the offences under section 48MA of *the Law* and section 74A of *The Terrorism Law*.

1.6. Structure and Content of the Handbook

19. This *Handbook* takes a two-level approach:

(a) Level one ("*Commission Rules*") sets out how *the Commission* requires the firm to meet the requirements of *Schedule 3*. Compliance with the *Commission Rules* will be taken into account by the courts when considering compliance with *Schedule 3* (which is legally enforceable and a contravention of which can result in prosecution); and
(b) Level two ("*guidance*") presents ways of complying with *Schedule 3* and the *Commission Rules*. The firm may adopt other appropriate and effective measures to those set out in *guidance*, including policies, procedures and controls established by the group Head Office of the firm, so long as it can demonstrate that such measures also achieve compliance with *Schedule 3* and the *Commission Rules*.

20. When the requirements of *Schedule 3* are explained or paraphrased in this *Handbook*, the term 'shall' is used and the text is presented in blue shaded boxes for ease of reference. Reference is also made to the relevant paragraph(s) of *Schedule 3*.

21. When the requirements of *the Transfer of Funds Ordinance* and *the EU Regulation* are explained or paraphrased in Chapter 14 of this *Handbook*, the term 'shall' is used and the text is presented in clear boxes for ease of reference. Reference is also made to the relevant paragraph(s) of the Ordinance.

22. Where the *Commission Rules* are set out, the term 'must' is used and the text is presented in red shaded boxes to denote that these are rules.

23. In all cases the terms 'shall' and 'must' indicate that these provisions are mandatory and subject to the possibility of prosecution (in the case of a contravention of *Schedule 3* or *the Transfer of Funds Ordinance*) as well as regulatory sanction and any other applicable sanctions.

24. In respect of *guidance*, this *Handbook* uses the terms 'should' or 'may' to indicate ways in which the requirements of *Schedule 3*, *the Transfer of Funds Ordinance* and the *Commission Rules* can be satisfied, but allowing for alternative means of meeting the requirements as deemed appropriate by the firm.

25. References to the *Commission Rules* within this *Handbook*, are made by stating the Chapter number, followed by the paragraph number, for example, Commission Rule 7.23 refers to the rule stated within Chapter 7 at paragraph 23. Sections have also been included within this *Handbook* for ease of navigation.

26. *The Commission* will from time to time update this *Handbook* to reflect new legislation, developments in the financial services and *PB* sectors, changes to international standards, recommendations from mutual evaluations, good practice and amendments to *Schedule 3* or *the Relevant Enactments*.

27. This *Handbook* is not intended to provide an exhaustive list of appropriate and effective policies, procedures and controls to counter *ML, TF* and *PF*. The structure of this *Handbook* is such that it permits the firm to adopt a *risk*-based approach appropriate to its particular circumstances. The firm should give consideration to additional measures which may be necessary to prevent any exploitation of it and of its products, services and/or delivery channels by persons seeking to carry out *ML, TF* and/or *PF*.

1.7. Significant Failure to Meet the Required Standards

28. For any firm, whether regulated by or registered with *the Commission*, the primary consequences of any significant failure to meet the standards required by *Schedule 3*, the *Commission Rules* and *the Relevant Enactments* will be legal ones. In this respect *the Commission* will have regard to the firm's compliance with the provisions of *Schedule 3*, the *Commission Rules* and *the Relevant Enactments* when considering whether to take enforcement action against it in respect of a breach of any requirements of the aforementioned. In such cases, *the Commission* has powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the licence of the firm where applicable.

29. Where the firm is regulated by *the Commission*, *the Commission* is entitled to take such failure into consideration in the exercise of its judgement as to whether the firm and its directors and managers have satisfied the minimum criteria for licensing. In particular, in determining whether the firm is carrying out its business with integrity and skill and whether a natural person is fit and

proper, *the Commission* must have regard to compliance with *Schedule 3*, the *Commission Rules* and *the Relevant Enactments*.

30. In addition, *the Commission* can take enforcement action under *the Enforcement Law*, *the Regulatory Laws* and/or *the Financial Services Commission Law* for any contravention of the *Commission Rules* where the firm is licensed under one or more of *the Regulatory Laws*.

31. Where the firm is not regulated by, but is registered with *the Commission*, *the Commission* is entitled to consider compliance with *Schedule 3*, the *Commission Rules* and *the Relevant Enactments* when exercising its judgement in considering the continued registration of the firm. In this respect *the Commission* can also take enforcement action under *the PB Law* where the firm is registered with *the Commission* under that law.

1.8. Data Protection

32. *The Bailiwick's* AML, CFT and CPF legislation requires the firm to collate and retain records and *documentation*. Where such records and *documentation* contain personal data, the firm will need to comply with the Data Protection (Bailiwick of Guernsey) Law, 2017 ("*the Data Protection Law*") which brings *the Bailiwick* into line with the European Union's ("EU") General Data Protection Regulation ("GDPR").

https://www.guernseylegalresources.gg/laws/guernsey-bailiwick/d/data-protection/data-protection-bailiwick-of-guernsey-law-2017-consolidated-text/
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679

1.9. The Financial Action Task Force

33. The FATF is an inter-governmental body that was established in 1989 by the ministers of its member jurisdictions. The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating *ML*, *FT*, *PF* and other related threats to the integrity of the international financial system.

34. *The FATF Recommendations* are recognised as the global AML, CFT and CPF standard. *The FATF Recommendations* therefore set an international standard which countries should implement through measures adapted to their particular circumstances. *The FATF Recommendations* set out the essential measures that countries should have in place to:

(a) identify risks and develop policies and domestic co-ordination;
(b) pursue *ML*, *FT* and *PF*;
(c) apply preventive measures for the financial sector and other designated sectors;
(d) establish powers and responsibilities for the competent authorities (for example, investigative, law enforcement and supervisory authorities) and other institutional measures;
(e) enhance the transparency and availability of beneficial ownership information of *legal persons* and *legal arrangements*; and
(f) facilitate international co-operation.

1.10. The National Risk Assessment

35. In accordance with *the FATF Recommendations*, *the Bailiwick*, led by the States of Guernsey's Policy & Resources Committee, undertakes a periodic "national" assessment of the ML, TF and PF risks to the Bailiwick. The first National Risk Assessment ("*NRA*"), published in 2020, was based on the methodology developed by the International Monetary Fund ("IMF") supplemented by additional information provided by the relevant agencies within *the Bailiwick* and industry to

ensure a thorough assessment of the *ML* and *FT risks* presented by the individual sectors within the finance industry and products and services from within *the Bailiwick*. New information and analysis, as well as an update on the 2020 assessment, was published in 2023 and included for the first time an assessment of the *PF risks* to the Bailiwick. An extension of the 2023 *NRA* was published in 2024 on *legal persons* and *legal arrangements*.

36. The key finding of the *NRA*s with regard to *ML risk* is that as an international finance centre with a low domestic crime rate, *the Bailiwick's* greatest *ML risk* comes from the laundering of the proceeds of foreign criminality largely through *legal persons* and *legal arrangements* which are used for cross-border business, holding or managing assets. The underlying offences most likely to be involved are bribery and corruption, fraud and tax evasion. The key finding of the *NRA*s with regard to *TF risks* is that the greatest *risks* come from its cross-border business being used to support foreign terrorism, by funds being passed through or administered from the *Bailiwick*. However, this *risk* is much lower than the *ML risks* from cross-border business. *TF* from cross-border business is most likely to arise in the context of secondary terrorist financing, i.e. where criminal proceeds are used to fund terrorism. The key finding of the more recent *NRA* with regard to *PF risks* is that the greatest *risks* come from its cross-border business being used for the movement of funds linked to proliferation activity, by funds being passed through or administered from the *Bailiwick*. However, as the *Bailiwick* has no diplomatic connections, and no known economic, geographic, ideological or political links with the two sanctioned countries for proliferation – the Democratic People's Republic of North Korea and Iran, this *risk* is more remote than the *TF risks* from cross-border business.

37. The assessment of *risks* and vulnerabilities detailed within an *NRA* will naturally cascade through to *specified businesses* within *the Bailiwick*. In this respect, references are made throughout *Schedule 3* and this *Handbook* requiring the firm to have regard to the content of the latest *NRAs* when undertaking certain activities, for example, the formulation of its *business risk assessments* and *risk appetite*.

38. *The Bailiwick* reviews the *NRAs* on an on-going and trigger-event basis, making changes as necessary taking into account market changes, the advancement of technology and data collected from industry, for example, through various surveys and regulatory returns.

39. All references to the *NRA* in the Handbook refer to the latest versions published by the States of Guernsey, including the 2024 assessment of *legal persons* and *legal arrangements*. A copy of *the Bailiwick's NRA*s can be found on the website of the States of Guernsey's Policy & Resources Committee:

National Risk Assessment

1.11 MONEYVAL

40. The Committee of Experts on the Evaluation of Anti-Money Laundering and the Financing of Terrorism ("MONEYVAL") is a monitoring body of the Council of Europe. The aim of MONEYVAL is to ensure that its member states have in place effective systems to counter *ML*, *TF* and *PF* and comply with the relevant international standards in these fields.

41. On 10 October 2012 the Committee of Ministers of the Council of Europe, following a request by the United Kingdom ("UK"), adopted a resolution to allow *the Bailiwick*, the Bailiwick of Jersey and the Isle of Man (the "*Crown Dependencies*") to participate fully in the evaluation process of MONEYVAL and to become subject to its procedures.

42. MONEYVAL's most recent evaluation of *the Bailiwick* was conducted during April 2024 and assessed *the Bailiwick's* compliance with the FATF 2012 Recommendations. In its report, published on 10 February 2025, MONEYVAL concluded that since the last evaluation in 2014

the Bailiwick has ‘made significant efforts to strengthen its legal and regulatory AML/CFT framework’ with a ‘robust AML/CFT legal framework for technical compliance’ aligned with the FATF Recommendations.

www.coe.int/en/web/moneyval/jurisdictions/guernesey

Chapter 2
Corporate Governance

Contents of this Chapter

2.1. Introduction

1. Good corporate governance should provide proper incentives for the *board* or senior management to pursue objectives that are in the interests of the firm and its shareholders and should facilitate effective monitoring of the firm for compliance with its AML, CFT and CPF obligations.

2. The Organisation for Economic Co-operation and Development ("OECD") describes the corporate governance structure of a firm as the distribution of rights and responsibilities among different participants, such as the *board*, managers and other stakeholders, and the defining of the rules and procedures for making decisions on corporate affairs.

3. The presence of an effective corporate governance system, within an individual company and across an economy as a whole, is key to building an environment of trust, transparency and accountability necessary for fostering long-term investment, financial stability and business integrity and helps to provide a degree of confidence that is necessary for the proper functioning of a market economy.

4. This Chapter, together with *Schedule 3*, provide a framework for the oversight of the policies, procedures and controls of the firm to counter *ML*, *TF* and *PF*.

5. In accordance with Paragraph 21(2) of *Schedule 3*, references in this Chapter and in the wider *Handbook* to the "*board*" shall mean the board of directors of the firm where it is a body corporate, or the senior management of the firm where it is not a body corporate (but is, for example, a partnership or a branch).

6. With reference to Paragraph 21(3) of *Schedule 3*, where the firm is a sole trader (for example, a personal fiduciary licence holder or a natural person registered as a *prescribed business* operating alone), references to the "*board*" are references to the natural person named in the licence or registration issued by *the Commission*, unless specified otherwise within this *Handbook*.

2.2. GFSC Code of Corporate Governance

7. The firm is expected to maintain good standards of corporate governance. In order to provide locally regulated *FSBs* and individual directors with a framework for sound systems of corporate governance and to help them discharge their duties efficiently and effectively, *the Commission* has issued the Finance Sector Code of Corporate Governance ("*the Code*").

   https://www.gfsc.gg/sites/default/files/inline-files/Finance%20Sector%20Code%20of%20Corporate%20Governance%202021.pdf

8. *The Code* is a formal expression of good governance practice against which *the Commission* can assess the degree of governance exercised over regulated persons. In this regard, *the Commission* is focussed on outcomes based regulation, i.e. *the Code* focuses on high-level principles which allow each firm to meet the requirements in a manner suitable to the specific *FSB's* business without having to adhere to prescriptive rules.

9. Whilst *the Code* does not apply to firms registered with *the Commission* under *the PB Law*, to partnerships, or to *Bailiwick* branches of foreign domiciled companies, its content can be helpful as a guide to *the Commission's* expectations when assessing compliance with this Chapter by those businesses.

2.3. Board Responsibility for Compliance

10. The *board* of the firm has effective responsibility for compliance with *Schedule 3* and the *Commission Rules*. References to compliance in this *Handbook* generally are to be taken as references to compliance with *Schedule 3* and the *Commission Rules*.

11. The *board* of the firm is responsible for managing the firm effectively and is in the best position to understand and evaluate all potential risks to the firm, including those of *ML*, *TF* and *PF*. The *board* must therefore take ownership of, and responsibility for, the *business risk assessments* and ensure that they remain up to date and relevant.

12. More information on the process and requirements for conducting *business risk assessments* can be found in Chapter 3 of this *Handbook*.

13. In accordance with Paragraphs 15(1)(b) and 16A of *Schedule 3*, and in addition to complying with the requirements of Paragraphs 1 to 14 of *Schedule 3*, the firm shall have policies, procedures and controls which have regard to the *ML*, *TF* and *PF risks* and the size of the business for the purposes of forestalling, preventing and detecting *ML*, *TF* and *PF*.

14. The *board* must organise and control the firm effectively, including establishing and *maintaining* appropriate and effective policies, procedures and controls as detailed below, and having adequate resources to manage and mitigate the identified *risks* of *ML*, *TF* and *PF* taking into account the size, nature and complexity of its business.

15. Taking into account the conclusions of the *business risk assessments*, in accordance with Paragraphs 2(b) and 16A of *Schedule 3*, the firm shall have in place effective policies, procedures and controls to identify, assess, mitigate, manage, review and monitor those *risks* in a way that is consistent with the requirements of *Schedule 3*, *the Relevant Enactments*, the *NRA* and the *Commission Rules* in this *Handbook*.

16. In addition to the general duty to understand, assess and mitigate *risks* as set out in Paragraph 2 of *Schedule 3* and the requirement to *maintain* effective policies, procedures and controls contained therein, the firm should be aware that other paragraphs of *Schedule 3* and this *Handbook* also contain more specific requirements in respect of the policies, procedures and controls required to mitigate particular *risks*, threats and vulnerabilities.

17. These policies, procedures and controls should enable the firm to comply with the requirements of *Schedule 3* and the *Commission Rules*, including amongst other things, to:

    (a) conduct, document and *maintain business risk assessments* to identify the inherent *ML*, *TF* and *PF risks* to the firm and to define the firm's AML, CFT and CPF *risk appetite* (see Chapter 3);
    (b) conduct *risk* assessments of all *business relationships* and *occasional transactions* to identify those to which Enhanced Customer Due Diligence ("*ECDD*") measures and monitoring must be applied, and those to which Simplified Customer Due Diligence ("*SCDD*") measures can be applied where this is considered appropriate (see Chapter 3);
    (c) apply sufficient Customer Due Diligence ("*CDD*") measures to identify, and verify the identity of, *customers*, *beneficial owners* and other *key principals*, whether natural persons, *legal persons* and *legal arrangements*, and to establish the purpose and intended nature of the *business relationship* or *occasional transaction* (see Chapters 4-7);
    (d) apply *ECDD* measures to those *business relationships* and *occasional transactions* deemed to pose a high *risk* of *ML*, *TF* or *PF* and/or *enhanced measures* to those *business relationships* or *occasional transactions* involving, or in relation to, one or more of the

higher *risk* factors prescribed by Paragraph 5(2) of *Schedule 3* sufficient to mitigate the specific *risks* arising (see Chapter 8);

(e) apply *SCDD* measures in an appropriate manner where the circumstances of a *business relationship* or *occasional transaction* are such that the *ML, TF* and *PF risks* have been assessed as low (see Chapter 9);

(f) conduct transaction and activity monitoring (see Chapter 11);

(g) monitor *business relationships* on a frequency appropriate to the assessed *risk* to ensure that any unusual, adverse or suspicious activity is highlighted and given additional attention (see Chapter 11);

(h) screen *customers*, *payees*, *beneficial owners* and other *key principals* to enable the prompt identification of any natural persons, *legal persons* or *legal arrangements* subject to United Nation ("UN"), UK or other sanction (see Chapter 12);

(i) report promptly to the *FIU* where an *employee* knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is involved in *ML, TF* and/or *PF* (including in connection with an attempted transaction) (see Chapter 13);

(j) screen transfers of *funds* for missing or incomplete *payer* and *payee* information where the firm is a payment service provider ("*PSP*") (see Chapter 14);

(k) screen potential *employees* to ensure the probity and competence of *board* and staff members (see Chapter 15);

(l) provide suitable and sufficient AML, CFT and CPF training to all *relevant employees*, identify those *employees* to whom additional training must be provided and provide such additional training (see Chapter 15);

(m) maintain records for the appropriate amount of time and in a manner which enables the firm to access relevant data in a timely manner (see Chapter 16);

(n) ensure that, where the firm is a majority owner or exercises control over a *branch office* or subsidiary established outside *the Bailiwick*, the *branch office* or subsidiary applies controls consistent with the requirements of *Schedule 3* or requirements consistent with *the FATF Recommendations*; and

(o) establish controls for ensuring compliance with *Schedule 3* and the rules in the *Handbook*, including a compliance monitoring programme and, where relevant, with regard to the *ML, TF* and *PF* risks, the size and nature of its business and rules and *guidance* in the *Handbook*, an independent audit function to evaluate the adequacy and effectiveness of its policies, procedures and controls.

2.4. Board Oversight of Compliance

18. The *board* is responsible for ensuring that the firm has policies, procedures and controls which are effective and proportionate to its *ML, TF* and *PF risks* and to the size and nature of its business. In determining the calibration of these policies, procedures and controls, the *board* should have regard not only to the firm's size, but to the inherent *ML, TF* and *PF risks* presented by the types of products and services it offers, its delivery channels and to the types of customers it has and their geographic connections. These factors should not be considered singly, but cumulatively in determining the appropriateness of its policies, procedures and controls. Essentially the higher the *ML, TF* and *PF risks* present through the nature of the firm's activities and customers, the more robust the control environment should be.

2.4.1. Independent Audit Function

19. In accordance with Paragraphs 15(1)(ba) and 16A of *Schedule 3*, the firm shall establish an independent audit function (where appropriate, having regard to the *ML, TF* and *PF risks*, and the size and nature, of the *specified business* in question), for the purpose of evaluating the adequacy and effectiveness of the policies, procedures and controls adopted by the *specified business* to comply with *Schedule 3*, *the Relevant Enactments* and the *Handbook*.

20. The independent audit function can be performed by an employee of the firm, but that employee should be independent from the firm's employees who apply its policies, procedures and controls. An employee who has designed the firm's policies, procedures and controls or is reviewing them within the Compliance Monitoring Programme ("CMP"), for example, the *MLCO*, would not be considered independent. Conversely, where a firm has separate individuals holding the *MLRO* position to that of the *MLCO*, the *MLRO* could feasibly perform the independent audit where they have not designed or reviewed the firm's policies, procedures and controls. An independent audit function will not look the same across all sectors, as different types of firms represent different types of *risk*. *Specified businesses* which are part of a large, potentially international, financial group are likely to maintain their own internal audit function, or utilise that of their group to periodically examine and evaluate their policies, procedures and controls and other *risk* management controls.

21. *Specified businesses* which have no internal or group audit function could use the services of a suitably skilled external person, provided that, whomever is chosen is conversant with *the Bailiwick*'s AML/CFT framework to examine and evaluate these controls. Where a firm utilises external services to fulfil the independent audit function, *the Commission* would expect the firm to apply the principles in the outsourcing guidance note issued by *the Commission* referenced in Section 2.5 of this *Handbook*, when considering the suitability of the proposed external party.

22. The firm must ensure that:

(a) the independent audit function examines and evaluates the adequacy and effectiveness of the policies, procedures and controls adopted by the firm to comply with *Schedule 3* and this *Handbook*;
(b) the independent audit function reports on and make recommendations to the *board* in relation to those policies, procedures and controls;
(c) if carried out by an internal or group audit function; that internal or group audit function monitors the firm's compliance with those recommendations; and
(d) if the independent audit is carried out by an external party that is unable to further monitor the firm's compliance with those recommendations; that responsibility for monitoring the firm's compliance with those recommendations is assigned to the *board*.

23. Where a suitably skilled external auditor undertakes, as part of an audit of the firm's annual financial statements, an assessment of the adequacy and effectiveness of the policies, procedures and controls within the firm on which they also report to the *board* either separately to or within the Management Letter, and the firm understands the scope of the audit undertaken, it could be regarded as an independent audit function where the *board* concludes the scope was adequate to meet this requirement. So too would the periodic engagement of a suitably skilled external compliance consultant, law firm or other third party to assess the quality of a firm's policies, procedures and controls and to report on that assessment to the *board*.

24. Where a firm establishes an internal audit function, the employees carrying out this function must be different to the employees who apply the firm's policies, procedures and controls on a general day-to-day basis.

25. A *specified business* must consider in combination all of the following factors when determining whether to have an independent audit function:

(a) whether the firm is operating in a higher *risk* sector as indicated by the *NRA*;
(b) the *risk* profile of its *customer* base, including that of any *specified businesses* which it manages or administers;
(c) the size of the firm, and

(d) any other significant factors which would affect *ML, TF* and *PF risk,* including, but not limited to:
   i. an acquisition and integration of another *specified business* or book of business; or
   ii. significant or recurring breaches identified during previous audits, through its compliance monitoring programme or by *the Commission.*

26. Where a firm is of a large size, and/or the inherent *ML, TF* and *PF risks* presented by the types of products and services it offers, its delivery channels, the types of customers it has and/or their geographic connections are of a higher *risk,* the firm should have a distinct and separate independent audit function. When assessing the firm's size consideration should be given to the number of customers and the value of the assets under management.

27. Within all sectors there can be higher *risk* firms arising from the size and/or nature of the customer base. Firms should consider these risks on both an individual and combined basis and not conclude the firm's *risk* solely on its size or rating attributed to their sector in the *NRA.*

28. An audit may cover all or part of a firm's policies, procedures and controls. It may occur annually or less frequently, for example every three years. An audit's frequency and scope will depend on whether audits are full, themed or targeted, the size and nature of the firm and its *risk* profile. Other factors will also be relevant for determining the frequency and scope of the audit, including whether the firm's compliance monitoring programme has identified significant or recurring breaches for which it would be prudent for an independent function to examine and evaluate remediation, or where the firm has acquired another *specified business* or significant book of business where an independent audit could confirm if it has been fully and properly integrated into the firm's business.

29. Where a firm does not have an independent audit function, whether internal or group, or where it has contracted no external party to undertake such an audit within the preceding three years, the *board* of the firm must consider on an annual basis whether it would be appropriate to commission an independent audit to examine and evaluate its policies, procedures and controls and, where the *board* considers it not to be appropriate, document the reasons for its decision. Such a decision should not be made solely on the basis that the size of the firm is too small.

30. A *specified business* which relies on the policies, procedures and controls of a *specified business* which is managing or administering it is required to take sufficient measures to meet these requirements. This may be met by relying on the independent audit function of its manager or administrator.

2.4.2. Compliance Monitoring Programme ("CMP")

31. In accordance with Paragraph 15(1)(c) of *Schedule 3*, the firm shall establish and *maintain* an effective policy, for which responsibility shall be taken by the *board*, for the review of its compliance with the requirements of *Schedule 3* and this *Handbook,* and such policy shall include provision as to the extent and frequency of such reviews.

32. The firm's policy for reviewing its compliance should set out how it will monitor its compliance with the requirements of *Schedule 3* and the rules in the *Handbook* i.e. establish the firm's CMP. Additionally the policy should set, where appropriate based upon *ML, TF* and *PF risks* and the firm's size, whether it should have an independent audit function to examine and evaluate its AML/CFT/CPF controls.

33. The *board* must consider the appropriateness and effectiveness of its compliance arrangements and its policy for the review of compliance at a minimum annually, or whenever material changes to the business of the firm or the requirements of *Schedule 3* or this *Handbook* occur. Where, as

a result of its review, changes to the compliance arrangements or review policy are required, the *board* must ensure that the firm makes those changes in a timely manner.

34. As part of its compliance arrangements, the firm is responsible for appointing an *MLCO* who is responsible for monitoring the firm's compliance with its policies, procedures and controls to forestall, prevent and detect *ML*, *TF* and *PF*. This Section should therefore be read in conjunction with Section 2.8.1. of this *Handbook* which sets out the roles and responsibilities of the *MLCO*.

35. In addition to appointing an *MLCO*, the *board* must ensure that the policy for the review of compliance takes into account the size, nature and complexity of the business of the firm, including the *risks* identified in the *business risk assessments*. The policy must include a requirement for sample testing of the effectiveness and adequacy of the firm's policies, procedures and controls.

36. The sample testing of the effectiveness and adequacy of the firm's policies, procedures and controls detailed above is often referred to as a CMP.

37. The *board* should take a *risk*-based approach when defining its compliance review policy and ensure that those areas deemed to pose the greatest *risk* to the firm are reviewed more frequently. In this respect the policy should review the appropriateness, effectiveness and adequacy of the policies, procedures and controls established in accordance with the requirements of *Schedule 3* and this *Handbook*. This includes, but is not limited to:

    (a) the application of *CDD* measures, including *ECDD*, *SCDD* and *enhanced measures*;
    (b) the Management Information ("MI") received by the *board*, including information on any *branch offices* and subsidiaries;
    (c) the management and testing of third parties upon which reliance is placed for the application of *CDD* measures, for example, via an *introducer* relationship or under an outsourcing arrangement;
    (d) the ongoing competence and effectiveness of the *MLRO*;
    (e) the handling of internal disclosures to the *MLRO* and external disclosures and any production orders or requests for information to or from the *FIU*;
    (f) the management of sanctions risks and the handling of sanctions notices;
    (g) the provision of AML, CFT and CPF training, including an assessment of the methods used and the effectiveness of the training received by *employees*; and
    (h) the policies, procedures and controls surrounding bribery and corruption, including both the *employees* and *customers* of the firm, for example, gifts and hospitality policies and registers.

38. In accordance with Paragraph 15(1)(d) of *Schedule 3*, the firm shall ensure that a review of its compliance with *Schedule 3* and this *Handbook* is discussed and minuted at a meeting of the *board* at appropriate intervals, and in considering what is appropriate, the firm shall have regard to the *risk* taking into account –

    (a) the size, nature and complexity of the firm,
    (b) its *customers*, products and services, and
    (c) the ways in which it provides those products and services.

39. The *board* may delegate some or all of its duties but must retain responsibility for the review of overall compliance with the AML, CFT and CPF requirements of *Schedule 3*, this *Handbook* and *the Relevant Enactments*.

40. Where the firm identifies any deficiencies as a result of its compliance review policy, it must take appropriate action to remediate those deficiencies as soon as practicable and give

consideration to the requirements of *Commission Rule* 2.63 where the deficiencies identified are considered to be serious or material.

41. Where the firm is managed or administered by another *specified business*, the responsibility for the firm and its compliance with *Schedule 3*, this *Handbook* and *the Relevant Enactments* is retained by the *board* of the managed or administered firm and not transferred to its manager or administrator.

2.5. Outsourcing

42. Where the firm outsources a function to a third party (either within *the Bailiwick* or overseas, or within its group or externally) the *board* remains ultimately responsible for the activities undertaken on its behalf and for compliance with the requirements of *Schedule 3*, this *Handbook* and *the Relevant Enactments*. The firm cannot contract out of its statutory and regulatory responsibilities to prevent and detect *ML*, *TF* and *PF*.

43. This Section should be read as referring to the outsourcing of any function relevant to the firm's compliance with its obligations under *Schedule 3*, this *Handbook* and *the Relevant Enactments*, for example, the appointment of a third party as the firm's *MLCO* or *MLRO*, or the use of a third party to gather the requisite *identification data* for the firm's *customers* and other *key principals*.

44. Where the firm is considering the outsourcing of functions to a third party, it should:

(a) review *the Commission's* guidance notes on outsourcing;
(b) consider implementing a terms of reference or agreement describing the provisions of the arrangement;
(c) ensure that the roles, responsibilities and respective duties of the firm and the outsourced service provider are clearly defined and documented;
(d) ensure that the *board*, the *MLRO*, the *MLCO*, other third parties and all *employees* understand the roles, responsibilities and respective duties of each party; and
(e) ensure that it has appropriate oversight of the work undertaken by the outsourced service provider.

45. Below are links to *the Commission's* guidance notes on the outsourcing of functions. While the documents are applicable only to those firms licensed under the Protection of Investors (Bailiwick of Guernsey) Law, 2020 ("*the POI Law*"), the Banking Supervision (Bailiwick of Guernsey) Law, 2020 ("*the Banking Law*") and the Insurance Business (Bailiwick of Guernsey) Law, 2002 ("*the IB Law*") respectively, the principles contained within are relevant across industry and provide a useful reference when considering an outsourcing arrangement:

https://www.gfsc.gg/sites/default/files/2021-10/Guidance%20Note%20on%20the%20Outsourcing%20of%20Functions%20by%20Entities%20Licensed%20Under%20The%20Protection%20of%20Investors%20%28Bailiwick%20of%20Guernsey%29%20Law%2C%202020.pdf
https://www.gfsc.gg/sites/default/files/Outsourcing-Risk-Guidance-Note-for-Banks.pdf
https://www.gfsc.gg/sites/default/files/20180711%20-%20Outsourcing%20Guidance.pdf

46. Prior to a decision being made to establish an outsourcing arrangement, the firm must make an assessment of the *risk* of any potential exposure to *ML*, *TF* and *PF* and must *maintain* a record of that assessment as part of its *business risk assessments*.

47. The firm should monitor the *risks* identified by its assessment of an outsourcing arrangement and review this assessment on an on-going basis in accordance with its *business risk assessment* obligations.

48. The firm should ensure, at the commencement of an outsourcing arrangement and on an ongoing basis, that:

    (a) the outsourced service provider:

        (i) has the appropriate knowledge, skill and experience;
        (ii) is cognisant of the applicable AML, CFT and CPF requirements;
        (iii) is sufficiently resourced to perform the required activities;
        (iv) has in place satisfactory policies, procedures and controls which are, and continue to be, applied to an equivalent standard and which are kept up to date to reflect changes in regulatory requirements and emerging *ML*, *TF* and *PF risks*; and
        (v) is screened and subject to appropriate due diligence to ensure the probity of the outsourced service provider;

    (b) the work undertaken by the outsourced service provider is monitored to ensure it complies with the requirements of *Schedule 3*, this *Handbook* and *the Relevant Enactments*;
    (c) any reports or progress summaries provided to the firm by the outsourced service provider contain meaningful, accurate and complete information about the activities undertaken, progress of work and areas of non-compliance identified; and
    (d) the reports received from the outsourced service provider explain in sufficient detail the materials reviewed and other sources investigated in arriving at its conclusions so as to allow the firm to understand how findings and conclusions were reached and to test or verify such findings and conclusions.

49. The fact that the firm has relied upon an outsourced service provider or the report of an outsourced service provider will not be considered a mitigating factor where the firm has failed to comply with a requirement of *Schedule 3*, this *Handbook* or *the Relevant Enactments*. The *board* should therefore ensure the veracity of any reports provided by an outsourced service provider, for example, by spot-checking aspects of such reports.

50. The firm must ensure that the outsourced service provider has in place procedures which include a provision that knowledge, suspicion, or reasonable grounds for knowledge or suspicion, of *ML*, *TF* and/or *PF* activity in connection with the outsourcing firm's business will be reported by the outsourced service provider to the *MLRO* of the outsourcing firm (subject to any tipping off provisions to which the outsourced service provider is subject) in a timely manner.

51. An exception to *Commission Rule* 2.50 would be where the outsourced service provider forms a suspicion that the outsourcing firm is complicit in *ML, TF* and/or *PF* activity. In such cases the outsourced service provider, where it is a *specified business*, must disclose its suspicion to the *FIU* in accordance with Chapter 13 of this *Handbook* and advise *the Commission* of its actions.

52. Where the firm chooses to outsource or subcontract work to an unregulated entity, it should bear in mind that it remains subject to the obligation to *maintain* appropriate policies, procedures and controls to prevent *ML, TF* and *PF*. In this context, the firm should consider whether such subcontracting increases the *risk* that it will be involved in, or used for, *ML, TF* and/or *PF*, in which case appropriate and effective controls to address that *risk* should be implemented.

2.6. Foreign Branches and Subsidiaries

53. In accordance with Paragraph 15(1)(e) of *Schedule 3*, the firm shall ensure that any of its *branch offices* and, where it is a body corporate, any body corporate of which it is the majority shareholder or control of which it otherwise exercises, which, in either case, is a *specified*

business in any country or territory outside *the Bailiwick* (collectively "its subsidiaries"), complies there with:

(i) the requirements of *Schedule 3* and this *Handbook*, and
(ii) any requirements under the law applicable in that country or territory which are consistent with *the FATF Recommendations*,

provided that, where requirements under (i) or (ii) above differ, the firm shall ensure that the requirement which provides the highest standard of compliance, by reference to *the FATF Recommendations*, is complied with.

54. In determining whether the firm exercises control over another entity, examples could include one or more of the following:

(a) where the firm determines appointments to the board or senior management of that entity;
(b) where the firm determines that entity's business model or *risk appetite*; and/or
(c) where the firm is involved in the day-to-day management of that entity.

55. In addition to the entities covered by Paragraph 2.53 above, in accordance with Paragraphs 15(1)(g) and 16A of *Schedule 3*, where the firm is an *FSB*, it shall ensure that the conduct of any agent that it uses is subject to requirements to forestall, prevent and detect *ML, TF* and *PF* that are consistent with those in *the FATF Recommendations* in respect of such an agent.

56. The AML, CFT and CPF programmes should incorporate the measures required under *Schedule 3*, should be appropriate to the business of its subsidiaries and should be implemented effectively at the level of those entities.

57. In accordance with Paragraphs 15(1)(f) and 16A of *Schedule 3*, the firm shall ensure that it and its subsidiaries effectively implement policies, procedures and controls in respect of the sharing of information (including but not limited to *customer*, *account* and transaction information) between themselves for the purposes of:

(a) carrying out *CDD*:
(b) sharing suspicions relating to *ML, TF* and *PF* that have been formed and reported to the *FIU* (unless the *FIU* has instructed that they should not be so shared), and
(c) otherwise forestalling, preventing and detecting *ML, TF* and *PF*,

whilst ensuring that such policies, procedures and controls protect the confidentiality of such information.

58. The policies, procedures and controls referenced above should ensure that adequate safeguards on the confidentiality and use of information exchanged between the firm and its subsidiaries are in place and that such sharing and use is subject to the provisions of the data protection legislation of the jurisdictions within which its subsidiaries are located.

59. In accordance with Paragraph 15(2) of *Schedule 3*, the obligations in Paragraphs 2.53 and 2.57 above apply to the extent that the law of the relevant country or territory allows and if the law of the country or territory does not so allow in relation to any requirement of *Schedule 3*, the firm shall *notify the Commission* accordingly.

60. In addition to advising *the Commission*, the firm should also ensure that appropriate controls are implemented to mitigate any *risks* arising related to the specific areas where compliance with appropriate AML, CFT and CPF measures cannot be met.

61. The firm must be aware that the inability to observe appropriate AML, CFT and CPF measures is particularly likely to occur in countries or territories which do not, or insufficiently apply, *the FATF Recommendations*. In such circumstances the firm must take appropriate steps to effectively deal with the specific *ML, TF* and *PF risks* associated with conducting business in such a country or territory.

62. Where the firm is a money service provider registered with *the Commission* in accordance with Schedule 4 to *the Law*, it must apply the requirements of this section where it uses agents to provide services on behalf of the firm, whether by contract or under the direction of the firm. It must also include these agents in its AML/CFT/CPF programmes and monitor them for compliance with these programmes.

2.7. Liaison with the Commission

63. The *board* of the firm must ensure that *the Commission* is notified of any material failure to comply with the provisions of *Schedule 3,* this *Handbook* or *the Relevant Enactments*, or of any serious breaches of the policies, procedures or controls of the firm.

64. The following are examples of the types of scenarios in which *the Commission* would expect to be *notified*. This list is not definitive and there may be other scenarios where *the Commission* would reasonably expect to be *notified*:

(a) the firm identifies, either through its compliance monitoring arrangements or by other means (for example, a management letter from an auditor), areas of material non-compliance where remediation work is required;
(b) the firm receives a report, whether orally or in writing, from an external party engaged to review its compliance arrangements, identifying areas of material non-compliance where remediation work is recommended;
(c) the firm receives a report from a whistle-blower and an initial or provisional investigation reveals some substance to the concerns raised;
(d) the firm is aware that an aspect of material non-compliance may have occurred across more than one member of its corporate group, including the firm (or the parent of the firm where it is a *branch office*), which may have a bearing on the firm's compliance with its AML, CFT and CPF obligations and/or the effectiveness of the firm's compliance arrangements;
(e) the firm discovers that the party to whom it has outsourced functions critical to compliance with *Schedule 3,* this *Handbook* or *the Relevant Enactments* has failed to apply one or more of the requirements of *Schedule 3*, this *Handbook* or *the Relevant Enactments* and remediation work is required;
(f) any aspect of material non-compliance identified involving a *business relationship* or *occasional transaction* with a *relevant connection* to a country listed in Appendix H to this *Handbook* and those covered by sanctions legislation applicable in *the Bailiwick*, regardless of the values involved; or
(g) any breach of the requirements placed upon the firm by *the Bailiwick's* sanctions framework, regardless of the number of *business relationships*/*occasional transactions* or values involved.

65. In addition to the above, *the Commission* would expect to be notified where the firm identifies a breakdown of administrative or control procedures (for example, a failure of a computer system) or any other event arising which is likely to result in a failure to comply with the provisions of *Schedule 3,* this *Handbook* and/or *the Relevant Enactments*.

66. *The Commission* recognises that from time to time the firm may identify instances of non-compliance as part of its ongoing monitoring or *relationship risk assessment* review programmes.

Provided that a matter meets the following criteria then *notification* to *the Commission* is not required:

(a) it is isolated in nature;
(b) it is readily resolvable within a short period of time;
(c) it does not pose a significant *risk* to the firm; and
(d) it does not compromise the accuracy of:

  (i) the *CDD information* held for the *customer*, *beneficial owner* or other *key principal*;
  (ii) the firm's understanding of the beneficial ownership of the *customer*; and
  (iii) the firm's understanding of the purpose and intended activity of the *business relationship*.

67. Notwithstanding that *notification* to *the Commission* is not required in the above circumstances, the firm should document its assessment of a matter and its conclusions as to why it is not considered to be material. *The Commission* reserves the right to enquire about such instances of non-compliance during on-site visits, thematic reviews and other engagements with the firm.

68. Where the firm has determined that a matter warrants *notification* to *the Commission*, *the Commission* would expect to receive early notice, even where the full extent of the matter is yet to be confirmed or the manner of remediation decided.

69. While not an exhaustive list, the following are examples of what *the Commission* considers to constitute poor practice in relation to a failure to *notify* it under *Commission Rule* 2.63:

(a) the firm lacks the resources to immediately address the non-compliance or seeks to undertake the necessary remediation work before *notifying the Commission*;
(b) the firm has found no evidence that an actual financial crime has occurred as a result of the non-compliance; or
(c) having identified a widespread weakness within its controls, the *board* decides to delay advising *the Commission* while it undertakes a full audit to assess the extent of the issue.

2.8. Key Persons

2.8.1. Money Laundering Compliance Officer

70. In accordance with Paragraph 15(1)(a) of *Schedule 3*, the firm shall, if it comprises more than one individual, appoint a person of at least manager level as the Money Laundering Compliance Officer ("*MLCO*") and provide the name, title and email address of that person to *the Commission* as soon as is reasonably practicable and, in any event, within fourteen days starting from the date of that person's appointment.

71. Notifications made in accordance with *Schedule 3* should be submitted via *the Commission's* PQ Portal:

https://online.gfsc.gg

72. The *MLCO* appointed by the firm must:

(a) be a natural person;
(b) be of at least manager level;
(c) have the appropriate knowledge, skill and experience to fulfil a compliance role within the firm;

(d) be employed by the firm or an entity within the same group as the firm (in the case of managed or administered businesses it is acceptable for an employee of the manager or administrator of the firm to be appointed as the *MLCO*); and
(e) be resident in the *British Islands*.

73. The firm must ensure that the *MLCO*:

(a) has timely and unrestricted access to the records of the firm;
(b) has sufficient resources to perform his or her duties;
(c) has the full co-operation of the firm's staff;
(d) is fully aware of his or her obligations and those of the firm; and
(e) reports directly to, and has regular contact with, the *board* so as to enable the *board* to satisfy itself that all statutory obligations and provisions in *Schedule 3*, this *Handbook* and *the Relevant Enactments* are being met and that the firm is taking sufficiently robust measures to protect itself against the potential *risk* of being used for *ML, TF* or *PF*.

74. As defined in Paragraphs 21(1) and 16A of *Schedule 3*, the *MLCO* appointed by the firm shall monitor compliance with policies, procedures and controls to forestall, prevent and detect *ML, TF* and *PF*.

75. In accordance with Section 2.3. above, the *board* is responsible for the firm's compliance with *Schedule 3* and this *Handbook*, including establishing appropriate and effective policies, procedures and controls to forestall, prevent and detect *ML, TF* and *PF*. By contrast, the *MLCO's* role is to monitor the firm's compliance with its policies, procedures and controls and periodically report thereon to the *board*. In this respect the functions of the *MLCO* include:

(a) overseeing the monitoring and testing of AML, CFT and CPF policies, procedures, controls and systems in place to assess their appropriateness and effectiveness;
(b) investigating any matters of concern or non-compliance arising from the firm's compliance review policy;
(c) establishing appropriate controls to mitigate any *risks* arising from the firm's compliance review policy and to remediate issues where necessary and appropriate in a timely manner;
(d) reporting periodically to the *board* on compliance matters, including the results of the testing undertaken and any issues that need to be brought to the *board's* attention; and
(e) acting as a point of contact with *the Commission* and to respond promptly to any requests for information made.

76. While it is not anticipated that the *MLCO* will personally conduct all monitoring and testing, the expectation is that the *MLCO* will have oversight of any monitoring and testing being conducted by the firm, for example, by a compliance team or an outsourcing oversight team, in accordance with the firm's compliance review policy.

77. The circumstances of the firm may be such that, due to the small number of *employees*, the *MLCO* holds additional functions or is responsible for other aspects of the firm's operations. Where this is the case, the firm must ensure that any conflicts of interest between the *MLCO* role and any other functions held are identified, documented and appropriately managed.

78. For the avoidance of doubt, the same individual can be appointed to the positions of Money Laundering Reporting Officer ("*MLRO*") and *MLCO*, provided the firm considers this appropriate having regard to the respective demands of the two roles and whether the individual has sufficient time and resources to fulfil both roles effectively.

2.8.2. Money Laundering Reporting Officer

79. In accordance with Paragraph 12(1)(a) of *Schedule 3*, the firm shall appoint a person of at least manager level as the *MLRO*, provide the name, title and email address of that person to *the Commission* as soon as is reasonably practicable and, in any event, within fourteen days starting from the date of that person's appointment, and ensure that all *employees* are aware of the name of that person.

80. In addition to *notifying the Commission*, in accordance with Paragraph 12(1)(d) of *Schedule 3*, the firm shall provide the name, title and email address of the *MLRO* to *the FIU* as soon as is reasonably practicable and, in any event, within fourteen days starting from the date of that person's appointment.

81. Notifications made in accordance with *Schedule 3* should be submitted via *the Commission's* PQ Portal:

https://online.gfsc.gg

82. The *MLRO* appointed by the firm must:

(a) be a natural person;
(b) be of at least manager level;
(c) have the appropriate knowledge, skill and experience;
(d) be employed by the firm or an entity within the same group as the firm (in the case of a managed or administered business it is acceptable for an *employee* of the manager or administrator to be appointed as the *MLRO*); and
(e) be resident in *the Bailiwick*.

83. The firm must ensure that the *MLRO*:

(a) is the main point of contact with the *FIU* in the handling of disclosures;
(b) has unrestricted access to the *CDD information* of the firm's *customers*, including the *beneficial owners* thereof;
(c) has sufficient resources to perform his or her duties;
(d) is available on a day-to-day basis;
(e) receives full co-operation from all staff;
(f) reports directly to, and has regular contact with, the *board* or equivalent of the firm; and
(g) is fully aware of both his or her personal obligations and those of the firm under *Schedule 3*, this *Handbook* and *the Relevant Enactments*.

84. The firm must provide the *MLRO* with the authority to act independently in carrying out his or her responsibilities under Part 1 of *the Disclosure Law* or Section 12, 15 or 15A of *the Terrorism Law*. The *MLRO* must be free to have direct access to the *FIU* in order that any suspicious activity may be reported as soon as possible. The *MLRO* must also be free to liaise with the *FIU* on any question of whether to proceed with a transaction in the circumstances.

2.8.3. Nominated Officer

85. In accordance with Paragraph 12(1)(b) (where the firm is an *FSB*) or 12(1)(c) (where the firm is a *PB*) of *Schedule 3*, the firm shall, if it comprises more than one individual, nominate a person to –

(a) receive disclosures, under Part I of *the Disclosure Law* and Section 12 or Section 15 of *the Terrorism Law* (a "*Nominated Officer*"), in the absence of the *MLRO, and*

(b) otherwise carry out the functions of the *MLRO* in that officer's absence,

and ensure that all *employees* are aware of the name of that *Nominated Officer*.

86. In accordance with Paragraph 12(1)(d) of *Schedule 3*, the firm shall provide the name, title and email address of any person nominated under Paragraphs 12(1)(b) or 12(1)(c) as set out above to the *FIU* as soon as is reasonably practicable and, in any event, within fourteen days starting from the date of that person's appointment.

87. The *Nominated Officer* must:

(a) be a natural person; and
(b) have the appropriate knowledge, skill and experience.

88. There is no obligation to advise *the Commission* of the name, title or email address of the *Nominated Officer* except for those firms licensed under *the Banking Law*. However, where the *Nominated Officer* is acting in place of the *MLRO* to cover an extended period of absence (for example, maternity leave, sabbatical or long-term sick leave) the firm should consider appointing the *Nominated Officer* as the *MLRO* on a temporary basis. Where this occurs *the Commission* should be notified in accordance with Section 2.8.2. above.

89. The firm must communicate the name of the *Nominated Officer* to all *employees* of the firm and ensure that all *employees* of the firm are aware of the natural person(s) to whom internal disclosures are to be made in the absence of the *MLRO*.

90. For the avoidance of doubt, in accordance with Paragraphs 12(1)(b)-(c) of *Schedule 3*, the requirements of this section do not apply where the firm comprises one individual, for example, a personal fiduciary licence holder and or a natural person registered as a *PB* and acting alone.

Chapter 3
Risk-Based Approach

Contents of this Chapter

3.1. Introduction

1. This Chapter is designed to assist the firm in taking a *risk*-based approach to the prevention of its products and services being used for the purposes of *ML, TF* and *PF* and is broken down into three main sections:

   (a) Risk-Based Approach - which provides a high-level overview of the *risk*-based approach;
   (b) Business Risk Assessments - which details the relevant requirements of *Schedule 3*, together with the *Commission Rules* and *guidance*, in respect of the firm undertaking *ML, TF* and *PF business risk assessments* and determining its *risk appetite*; and
   (c) Relationship Risk Assessments - which sets out the relevant obligations of *Schedule 3*, together with the *Commission Rules* and *guidance*, for the conducting of *risk* assessments of new and existing *business relationships* and *occasional transactions*.

Risk-Based Approach

3.2. Definition, Purpose and Benefits

2. A *risk*-based approach towards the prevention and detection of *ML, TF* and *PF* aims to support the development of preventative and mitigating measures that are commensurate with the *ML, TF* and *PF risks* identified by the firm and to deal with those *risks* in the most cost-effective and proportionate way. The *PF risks* to a firm relate solely to the breach of targeted financial sanctions that are imposed under any international sanctions measure that has been implemented in *the Bailiwick* and relate to the proliferation of weapons of mass destruction and its financing, and for the avoidance of doubt, the breach of targeted financial sanctions includes their non-implementation, circumvention or evasion. At a minimum, firms must assess their risk of breaching targeted financial sanctions implemented in *the Bailiwick* in order to comply with *Schedule 3* and the *Handbook*, but depending on the nature, scale and complexity of their business, firms may wish to undertake a wider risk assessment of *proliferation financing* in line with the *PF* guidance issued by the States of Guernsey.

3. Paragraphs 2 and 16A of *Schedule 3* provides a general duty for the firm to understand, assess and mitigate *risks*. In this respect the firm shall:

   (a) Understand its *ML, TF* and *PF risks*; and
   (b) have in place effective policies, procedures and controls to:

      (i) identify,
      (ii) assess,
      (iii) mitigate,
      (iv) manage, and
      (v) review and monitor,

   those *risks* in a way that is consistent with the requirements of *Schedule 3, the Relevant Enactments*, the requirements of this *Handbook* and the *NRA*.

4. A *risk*-based approach prescribes the following procedural steps to manage the *ML, TF* and *PF risks* faced by the firm:

   (a) identifying the specific threats posed to the firm by *ML, TF* and *PF* and those areas of the firm's business with the greatest vulnerability;
   (b) assessing the likelihood of those threats occurring and the potential impact of them on the firm;

(c) mitigating the likelihood of occurrence of identified threats and the potential for damage to be caused, primarily through the application of appropriate and effective policies, procedures and controls;
(d) managing the residual *risks* arising from the threats and vulnerabilities that the firm has been unable to mitigate; and
(e) reviewing and monitoring those *risks* to identify whether there have been any changes in the threats posed to the firm which necessitate changes to its policies, procedures and controls.

5. In applying a *risk*-based approach and taking the steps detailed above, it is crucial that, regardless of the specific considerations and actions of the firm, clear documentation is prepared and retained to ensure that the *board* and senior management can demonstrate their compliance with the requirements of *Schedule 3* and the *Commission Rules* in this *Handbook*.

6. A *risk*-based approach starts with the identification and assessment of the *risk* that has to be managed. In the context of *Schedule 3* and this *Handbook*, a *risk*-based approach requires the firm to assess the *risks* of how it might be involved in *ML, TF* and *PF*, taking into account its *customers* (and the *beneficial owners* of *customers*), countries and geographic areas, the products, services and transactions it offers or undertakes, and the delivery channels by which it provides those products, services and/or transactions.

7. In determining how the *risk*-based approach should be implemented, the firm should analyse and seek to understand how the identified *ML, TF* and *PF risks* affect its business. This determination should take into account a range of information, including (amongst others) the type and extent of the *risks* that the firm is willing to accept in order to achieve its strategic objectives (its "*risk appetite*"), its AML, CFT and CPF experience and *the Bailiwick's NRA*.

8. Through the *business risk assessments* and determination of a *risk appetite*, the firm can establish the basis for a *risk*-sensitive approach to managing and mitigating *ML, TF* and *PF* risks. It should be noted, however, that a *risk*-based approach does not exempt the firm from the requirement to apply *enhanced measures* where it has identified higher *risk* factors as detailed in Chapter 8 of this *Handbook*.

9. *Schedule 3* and this *Handbook* do not prohibit the offering of any products or services or the acceptance of any *customer*, unless it is known, or there are reasonable grounds to suspect, that the *customer*, or the *beneficial owner* thereof, is undertaking or associated with *ML, TF* or *PF*. The *risk*-based approach, as defined in *Schedule 3* and this *Handbook*, instead requires that the *risks* posed by *customers* (and the *beneficial owners* of *customers*), countries and geographic areas, products, services, transactions and delivery channels are identified, assessed, managed and mitigated and that evidence of such is documented and reviewed on an on-going basis.

10. By adopting a *risk*-based approach the firm should ensure that measures to prevent or mitigate *ML, TF* and *PF* are commensurate with the *risks* identified. In this respect, the *business risk assessments* will also serve to enable the firm to make decisions on how to allocate its resources in the most efficient and effective way and to determine its appetite and tolerance for *risk*.

11. No system of checks will detect and prevent all *ML, TF* and *PF*. A *risk*-based approach will, however, serve to balance the cost burden placed upon the firm and its *customers* with a realistic assessment of the threat of the firm being used in connection with *ML, TF* and/or *PF*. It focuses the effort where it is needed and has most impact.

12. The benefits of a *risk*-based approach include:

(a) recognising that the *ML, TF* and *PF* threats to the firm vary across its *customers*, countries/geographic areas, products/services and delivery channels;

(b) providing for the *board* to apply its own approach to the policies, procedures and controls of the firm in particular circumstances, enabling the *board* to differentiate between its *customers* in a way that matches the *risk* to its particular business;
(c) helping to produce a more cost-effective system of *risk* management;
(d) promoting the prioritisation of effort and activity by reference to the likelihood of *ML, TF* and/or *PF* occurring;
(e) reflecting experience and proportionality through the tailoring of effort and activity to *risk*;
(f) enabling the application of the requirements of *Schedule 3* and this *Handbook* sensibly and in consideration of all relevant *risk* factors; and
(g) allowing for the consideration of the accumulation of identified *risks* and the determination of the level of overall *risk*, together with the appropriate level of mitigation to be applied.

13. It is important to acknowledge that various sectors and types of business, whether in terms of products/services, delivery channels or types of *customers*, can differ materially. An approach to preventing *ML, TF* and *PF* that is appropriate in one sector may be inappropriate in another. Appendix D to this *Handbook* provides *guidance* on sector-specific *risk* factors to assist the firm in the development of its *risk* management framework.

3.3. Identification and Mitigation of Risks

14. *Risk* can be seen as a function of three factors and a *risk* assessment involves making judgements about all three of the following elements:

(a) threat – a person or group of persons, an object or an activity with the potential to cause harm;
(b) vulnerability – an opportunity that can be exploited by the threat or that may support or facilitate its activities; and
(c) consequence – the impact or harm that *ML, TF* and *PF* may cause.

15. Having identified where it is vulnerable and the threats that it faces, the firm should take appropriate steps to mitigate the opportunity for those *risks* to materialise. This will involve determining the necessary controls or procedures that need to be in place in order to reduce the *risks* identified. The documented *risk* assessments that are required to be undertaken by *Schedule 3* will assist the firm in developing its *risk*-based approach.

16. In accordance with Paragraph 3(7) of *Schedule 3*, the firm shall have regard to:

(a) any relevant *Commission Rules* and *guidance* in this *Handbook*,
(b) any relevant notice or instruction issued by *the Commission* under *the Law*, and
(c) the *NRA*,

in determining what constitutes high or low *risk*, what its *risk appetite* is, and what constitute appropriate measures to manage and mitigate *risks*.

17. In addition to those noted above, information on *ML, TF* and *PF risk* factors could come from a variety of other sources, whether these are accessed individually or through commercially available tools or databases that pool information from several sources. The sources could include:

(a) national and supranational *risk* assessments, such as those published by the UK, the EU and other countries or territories similar to *the Bailiwick*;
(b) information published by law enforcement agencies (for example, the *FIU*) such as threat reports, alerts and typologies;
(c) information published by *the Commission*, such as thematic reports, warnings and the reasoning set out in enforcement actions taken by it;

(d) information on the purpose and rationale of UN, UK and other sanctions regimes;
(e) Guidance on *ML*, *TF* and *PF* published by the States of Guernsey Policy and Resources Committee;
(f) information from international standard-setting bodies, including the FATF, such as guidance papers and reports on specific threats or *risks*, as well as mutual evaluation reports when considering the *risks* associated with a particular country or geographic area;
(g) information provided by industry bodies, such as typologies and emerging *risk*s;
(h) information published by non-governmental organisations (for example, Global Witness or Transparency International); and
(i) information published by credible and reliable commercial sources, (for example, *risk* and intelligence reports) or open sources (for example, reputable newspapers).

18. Retaining *documentation* on the results of the firm's *risk* assessment framework will assist the firm to demonstrate how it:

(a) identifies and assesses the *risks* of being used for *ML*, *TF* and *PF*;
(b) agrees and implements appropriate and effective policies, procedures and controls to manage and mitigate *ML*, *TF* and *PF risk*;
(c) monitors and improves the effectiveness of its policies, procedures and controls; and
(d) ensures accountability of the *board* in respect of the operation of its policies, procedures and controls.

3.4. Accumulation of Risk

19. In addition to the individual consideration of each *risk* factor, the firm must also consider all such factors holistically to establish whether their concurrent or cumulative effect might increase or decrease the firm's overall *risk* exposure and the dynamic that this could have on the controls implemented by the firm to mitigate *risk*.

20. Such an approach is relevant not only to the firm in its consideration of the *risks* posed to its business as a whole as part of undertaking its *business risk assessments*, but also in the consideration of the *risk* that individual *business relationships* or *occasional transactions* pose.

21. There are also other operational factors which may increase the overall level of *risk*. These factors should be considered in conjunction with the firm's *ML*, *TF* and *PF risks*. Examples of such factors could be the outsourcing of AML, CFT and CPF controls or other regulatory requirements to an external third party or another member of the same group as the firm; or the use of on-line or web-based services and cyber-crime risks which may be associated with those service offerings.

3.4.1. Weighing Risk Factors

22. In considering the *risk* of a *business relationship* or *occasional transaction* holistically, the firm may decide to weigh *risk* factors differently depending on their relative importance.

23. When weighing *risk* factors, the firm should make an informed judgement about the relevance of different *risk* factors in the context of a *business relationship* or *occasional transaction*. This will likely result in the firm allocating varying 'scores' to different factors; for example, the firm may decide that a *customer's* personal links to a country, territory or geographic area associated with higher *ML*, *TF* and/or *PF risk* is less relevant in light of the features of the product they seek.

24. Ultimately, the weight given to each *risk* factor is likely to vary from product to product and *customer* to *customer* (or category of *customer*). When weighing *risk* factors, the firm should ensure that:

(a) the *risk* rating is not unduly influenced by just one *risk* factor;
(b) economic or profit considerations do not influence the *risk* rating;
(c) the weight assigned does not lead to a situation where it is impossible for any *business relationship* or *occasional transaction* to be classified as a *high risk relationship*;
(d) the provisions of Paragraph 5(1) of *Schedule 3* setting out the situations which will always present a high *risk* (for example, the involvement of *foreign PEPs* or *correspondent banking relationships*) cannot be over-ruled; and
(e) it is able to override any automatically generated *risk* scores where necessary. The rationale for the decision to override such scores should be documented appropriately.

25. Where the firm uses automated IT systems to allocate overall *risk* scores to *business relationships* or *occasional transactions* and does not develop these in house but purchases them from an external provider, it should understand how the system works and how it combines *risk* factors to achieve an overall *risk* score. The firm should be able to satisfy itself that the scores allocated reflect the firm's understanding of *ML, TF* and *PF risk* and it should be able to demonstrate this.

3.5. Policies, Procedures and Controls

26. In accordance with Paragraph 3(6) of *Schedule 3*, the firm shall –

(a) have in place policies, procedures and controls approved by its *board* that are appropriate and effective, having regard to the assessed *risk*, to enable it to mitigate and manage:

(i) *risks* identified in the *business risk assessments*, and *relationship risk assessments* undertaken under Paragraph 3(4)(a) of *Schedule 3*; and
(ii) *risks* relevant, or potentially relevant, to the firm identified in the *NRA* (which *risks* shall be incorporated into the *business risk assessments*);

(b) regularly review and monitor the implementation of those policies, controls and procedures and enhance them if such enhancement is necessary or desirable for the mitigation and management of those *risks;* and
(c) take additional measures to manage and mitigate higher *risks* identified in the *business risk assessments* and in *relationship risk assessments* undertaken under Paragraph 3(4)(a) of *Schedule 3*.

27. The firm's policies, procedures and controls must take into account the nature and complexity of the firm's operation, together with the *risks* identified in its *business risk assessments*, and must be sufficiently detailed to allow the firm to demonstrate how the conclusion of each *relationship risk assessment* has been reached.

Business Risk Assessments

3.6. Introduction

28. A key component of a *risk*-based approach involves the firm identifying areas where its products and services could be exposed to the *risks* of *ML, TF* and *PF* and taking appropriate steps to ensure that any identified *risks* are managed and mitigated through the establishment of appropriate and effective policies, procedures and controls.

29. The *business risk assessments* are designed to assist the firm in making such an assessment and provide a method by which the firm can identify the extent to which its business and its products and services are exposed to *ML, TF* and *PF*. Good quality *business risk assessments* are therefore vital for ensuring that the firm's policies, procedures and controls are proportionate and targeted appropriately.

30. The *board* must ensure that the firm's *business risk assessments*, together with details of the firm's *risk appetite*, are communicated to all *relevant employees*.

31. In communicating the firm's *business risk assessments* and *risk appetite*, the firm should ensure that *relevant employees* understand the implications of these on the day-to-day functions of *relevant employees* and their effect on the strategic objectives of the firm, in particular those *relevant employees* with *customer*-facing or business development roles.

3.7. Content and Structure

32. In accordance with Paragraphs 3(1)(a) and 16A of *Schedule 3*, the firm shall carry out and *document* a suitable and sufficient *ML business risk assessment*, a suitable and sufficient *TF business risk assessment* and a suitable and sufficient *PF business risk assessment*, which are specific to the firm.

33. In carrying out the *business risk assessments* in accordance with Paragraphs 3(1) and 16A of *Schedule 3*, the firm must ensure that the assessments of the *risks* of *ML*, *TF* and *PF* are distinct from one another, clearly addressing the different threats posed by each *risk* and should reflect that appropriate steps have been taken in order to identify and assess the specific *risks* posed to the firm.

34. The format of the *business risk assessments* is a matter to be decided by the firm. However, regardless of the format used, it is important that the *business risk assessments* are *documented* in accordance with Paragraph 3(1)(a) of *Schedule 3* in order to provide clear evidence to demonstrate the basis upon which they have been conducted. Notwithstanding the requirement for the *ML*, *TF* and *PF business risk assessments* to be distinct, there is nothing to prevent them being contained within one over-arching *document* recording, in its entirety, the firm's assessment of *ML*, *TF* and *PF risk.*

35. In accordance with Paragraphs 3(3) and 16A of *Schedule 3*, the *business risk assessments* shall be appropriate to the nature, size and complexity of the firm, and be in respect of:

(a) *customers*, and the *beneficial owners* of *customers*,
(b) countries and geographic areas, and
(c) products, services, transactions and delivery channels (as appropriate), and in particular in respect of the *ML*, *TF* or *PF risks* that may arise in relation to:

(i) the development of new products and new business practices, before such products are made available and such practices adopted; and
(ii) the use of new or developing technologies for both new and pre-existing products, before such technologies are used and adopted,

and the *business risk assessments* must include (without limitation) consideration of the implications for, and risks to, the business of the offences specified in the *NRA* as being the most likely predicate offences of *the Bailiwick* being used for *money laundering, terrorist financing* or *proliferation financing*.

36. The *business risk assessments* must take account of the findings of the *NRA* and reflect the firm's assessment of whether the *risks* identified in the *NRA* are relevant, or potentially relevant, to the firm, and where they are, identify the measures for mitigating those *risks*. All *business risk assessments* must consider the greatest *ML*, *TF* and *PF risks* identified within the *NRA*, including the predicate offences most likely to be involved in *ML*, *TF* or *PF*, specifically bribery and corruption, fraud, and tax evasion.

37. The firm should have regard to the *ML*, *TF* and *PF* threats relevant to its sector as articulated in the latest *NRA*, assess how those threats are relevant to the products and services it offers, and assess its vulnerability to *ML*, *TF* and *PF* after taking into account mitigating measures. The sections of the *NRA* which discuss the modalities of *ML*, and *TF*, and the case studies contained within, are particularly relevant. The assessment of *PF risks* should be focused on the breach, non-implementation, circumvention or evasion of international sanction measures implemented in the Bailiwick which relate to *PF* in respect of sub-paragraph 3(3)(a) to (c) of *Schedule 3*.

38. Despite there being no *TF* or *PF* case studies in the *NRA*, some of the countries and patterns of behaviour involved in the case studies on sanctions and *ML* case studies will be relevant to possible *TF* and *PF* activity, especially in relation to secondary *TF* or *PF* i.e. where the proceeds of crime are used to fund terrorism or proliferation. Additionally the firm should have regard to *TF* and *PF* typologies issued by the FATF.

FATF TF Guidance
FATF PF Guidance
FATF PF Typology

39. In accordance with Paragraph 3(2) of *Schedule 3*, in carrying out its *business risk assessments*, the firm shall consider all relevant *risk* factors before determining:

(a) the level of overall *risk* to the firm;
(b) the firm's *risk appetite*; and
(c) the appropriate level and type of mitigation to be applied.

40. The *business risk assessments* should contain references as to how the firm manages or mitigates the *risks* which it has identified and the policies, procedures and controls which have been established in this regard.

41. Industry sectors will have inherent and/or generic *risk* factors and these should be referenced in the firm's *business risk assessments*. *Business risk assessments* are likely to be deficient if the *risks* to the firm's sector identified in the *NRA* are not considered or if the irrelevance of those *risks* to its business is not explained in the assessments. Additionally, the firm will also have *risk* factors particular to its own business which should be analysed in the *business risk assessments*.

42. The firm must not copy the *business risk assessments* prepared by another business, or use 'off-the-shelf' assessments which pre-identify suggested *ML*, *TF* and *PF risks* without the firm ensuring the assessments have been tailored to its business and the specific *risks* that it faces.

43. Such an approach in adopting an 'off-the-shelf' assessment can lead to the firm failing to accurately identify the *ML*, *TF* and *PF risks* specific to its business. This in turn can lead to inadequate or inappropriate policies, procedures and controls that are either ill-suited to the firm or fail to appropriately mitigate the firm's *risks*.

44. In addition to the above, the *business risk assessments* should not:

(a) be a 'cut and paste' version of the relevant sections of the *Handbook* and/or the *NRA*. This does not demonstrate that the *board* has given serious consideration to the vulnerabilities specific to the products, services and *customers* of the firm;
(b) be generic assessments which have simply been populated with general information. Again, this does not demonstrate that the *board* has given serious consideration to the vulnerabilities particular to its business;
(c) contain unsubstantiated, highly generalised references to the *risks* faced by the firm, for example, a reference to all business being low *risk* or statements such as 'there is a risk that our products could be used to finance terrorism'. Such statements would not be

acceptable unless they are backed-up with specific information evidencing how this assessment had been made;

(d) copy statements about a sector's *risks* from the *NRA* without substantiating why those *risks* are relevant (or not relevant) to the firm; or

(e) focus upon isolated *risk* factors, for example, concentrating solely upon a geographic location.

45. There may be occasions where threats span a number of *risk* categories, for example, there may be operational risks associated with a piece of *customer*-facing technology in addition to *ML, TF* and *PF* or other financial crime risks. Where the firm wishes to combine its *ML, TF* and *PF business risk assessments* with assessments of other risks, such as conduct risk or credit risk, the firm should ensure that the assessments of *ML, TF* and *PF risk* are clearly identified.

3.8. Risk Appetite

46. In accordance with Paragraph 3(2) of *Schedule 3* the firm shall, having considered all relevant *risk* factors, determine its *risk appetite* as part of carrying out its *business risk assessments*.

47. The determination of the firm's *risk appetite* is an important element in carrying out its *business risk assessments*, setting out the amount of *ML, TF* and *PF risk* it is prepared to accept in pursuing its strategic objectives. Having identified the inherent *ML, TF* and *PF risks* to its business, identifying the amount of such *risk* that it is willing to take on is an integral part of the design and implementation of appropriate and effective policies, procedures and controls to manage and mitigate *risk*.

48. The *board* is responsible for setting the firm's *risk appetite*, together with the overall attitude of the firm to *risk* taking. The primary goal of the *risk appetite* is to define the amount of *risk* that the firm is willing to accept in the pursuit of its objectives, as well as outlining the boundaries of its *risk* taking, beyond which the firm is not prepared to accept *risk*.

49. In this respect the firm's documented *risk appetite* should include a qualitative statement (for example, detailing those categories of *customer* or country/territory that the firm deems to pose too great a *risk*) as well as quantitative measures to support its *risk appetite*, including the firm's tolerance and capacity to take on *risk*, i.e. the maximum level of *risk* that it is possible to accept without exceeding or overstretching its administrative, operational and resourcing constraints.

50. In determining its *risk appetite* the firm should be realistic in the context of its business model. A firm targeting business from high *risk* countries or territories, offering high *risk* products or services or with a large percentage of *high risk relationships* would consequently have a high *risk appetite* and its *business risk assessments* should be drafted accordingly.

51. The following is a non-exhaustive list of example questions that the firm could consider in developing its *risk appetite*:

(a) What are the strategic objectives of the firm? Are they clear?
(b) What specific *risks* could pursuing these objectives expose the firm to?
(c) How relevant to the firm's objectives are the main *risks* to the firm's sector that have been identified in the *NRA?*
(d) What are the significant *risks* the *board* is willing to take?
(e) What are the significant *risks* the *board* is not willing to take?
(f) Is the *board* clear about the nature and extent of the significant *risks* it is willing to take in achieving its strategic objectives?
(g) Have the *board* and senior management reviewed the capabilities of the firm to manage the *risks* that it faces?
(h) What capacity does the firm have in terms of its ability to manage *risks*?

(i) Do *employees* of the firm understand their role and responsibility for managing *risk*?
(j) How much does the firm spend on compliance and *risk* management each year? How much does the firm need to spend to ensure its compliance and *risk* management controls can sufficiently mitigate the identified *risks*?

3.9. Review

52. In accordance with Paragraph 3(1)(b) of *Schedule 3*, the firm shall regularly review its *business risk assessments*, at a minimum annually and more frequently when changes to the business of the firm occur, so as to keep them up to date.

53. The *NRA* process is an iterative one, which will involve the exercise being repeated over time. Therefore, the firm must take into account the findings of any updated *NRA* and reflect the firm's assessment of whether the *risks* identified in any updated *NRA* are relevant, or potentially relevant, to the firm, and where they are, identify the measures for mitigating those *risks*. This must form part of the next review (which must occur at a minimum of annually) of the firm's *business risk assessment*, unless *the Commission* calls upon firms to do this sooner.

54. When a firm reviews its *business risk assessments*, the fact that the review occurred should be recorded.

55. Just as the activities of the firm can change, so too can the corresponding *ML, TF* and *PF risks*. Mergers, acquisitions, the purchase or sale of a book of business, the adoption of a piece of technology or technological solution, the introduction of a new product or service, a restructuring or a change of external service provider are just some of the events which can affect both the type and extent of the *risks* to which the firm could be exposed. In light of any such changes the *business risk assessments* should be reviewed to consider whether the *risks* to the firm have changed and to ensure that the controls to mitigate those *risks* remain effective.

56. Other operational changes, for example, a change in *employee* numbers or a change to group policies, can all have an impact upon the resources required to effectively manage *ML, TF* and *PF risks*.

57. Where, as a result of the firm's review, changes to the *business risk assessments* are required, in accordance with Paragraph 3(1)(b) of *Schedule 3* the firm shall make those changes.

58. Where changes to the *business risk assessments* are made, the firm must give consideration to whether the policies, procedures and controls of the firm remain appropriate and effective in light of the revised *business risk assessments* and make any changes it considers appropriate in a timely manner.

3.10. Example Risk Factors

59. *The Bailiwick*'s primary *ML risks* identified within the *NRA* come from the laundering of the *proceeds* of foreign criminality. The underlying, or "predicate", offences most likely to be involved are bribery and corruption, fraud and tax evasion. Below are example *risk* factors linked to these predicate offences derived from the *NRA* and the FATF to assist firms in undertaking their *business risk assessments*.

60. Bribery and corruption *risk*:

General *risk* factors

(a) Kleptocracy (theft of state assets by heads of state or senior executives of state-owned enterprises);
(b) Manipulation of the procurement process by *PEP*s in favour of certain individuals or entities; and
(c) Infrastructure projects, including utilities and public service procurement, or the sale of state owned assets and infrastructure;

Customer risk factors:

(d) *Customers* and *beneficial owners* assessed as *PEP*s who are connected to countries or territories regarded as having higher corruption *risk*;
(e) *Business relationships* that are connected to sensitive industries linked to higher corruption *risks*, for example, due to their dependence on government awards of contracts, licences, permits and/or rights, or to countries with poor economic situations;
(f) The involvement of *foreign PEP*s, whether as a *customer* directly or indirectly, especially where the *foreign PEP has/had*:
    i. influence over significant state assets and *funds* (including state owned enterprises), policies and/or operations, or;
    ii. control over regulatory approvals, or;
    iii. the ability to control or interfere with mechanisms established to prevent and detect *ML*, *TF* and/or *PF*.
(g) The holding or management of assets that result from or are otherwise linked to illicit enrichment by *PEP*s;
(h) Credible allegations of corruption or bribery against a *key principal* (including when criminal charges have not been brought);
(i) *Customers* and *beneficial owners* who are potentially more junior public officials, particularly with an important role in significant procurement, export contracts, licensing and other activities with substantial economic consequences for the interest of their political parties particularly in connection with a higher *risk* jurisdiction;
(j) *Key principals* who appear to be acting on the instruction of additional, undeclared parties;
(k) The use of corporate vehicles, where the reasons for their use is unclear and which obfuscates the identity of the parties involved, such as the *beneficial owner*;
(l) Whether the corporate vehicle structures are particularly or unusually complex and no clear and sound rationale is evident for the level of complexity involved;
(m) The use of intermediaries who have no effective AML/CFT/CPF controls, or are based in unregulated, poorly regulated, or otherwise high *risk* jurisdictions;
(n) The involvement of public procurement activities in sensitive industries, such as the defence industry, the extractive industries, human health activities/pharmaceutical and medical device companies, large infrastructure projects, including public works contracts and construction;
(o) Connections to privatisation and/or developmental assistance in developing countries;
(p) Professional enablers of economic/financial crime, such as lawyers or finance experts whose wilful, complicit or negligent conduct may facilitate *ML*, *TF* and *PF* and other financial crime, who are associated with *PEP*s;
(q) Complex ownership structures, the reasons for which are unclear;
(r) Use of multiple jurisdictions, the reasons for which are unclear; and
(s) Sham agreements in general, but are also particularly likely to arise with procurement relating to military equipment and infrastructure.

Countries and territories *risk* factors:

(t) Relevant connections to jurisdictions associated with higher levels of bribery and corruption;
(u) Whether financial disclosures by public officials are mandated within higher risk jurisdictions which may reduce the *risk*;
(v) Whether governmental contracts within higher risk jurisdictions are disclosed and procurement processes are transparent which may reduce the *risk*;
(w) *Business relationships* or *occasional transactions* connected with unregulated, poorly regulated or otherwise high *risk* jurisdictions; and
(x) A country or territory that scores poorly on corruption perception indices.

Product, service, transaction or delivery channel *risk* factors which are more vulnerable:

(y) Private banking due to the prevalence of high net worth *customers* and the bespoke nature and complexity of some of the types of products and services available;
(z) Anonymous transactions (which may include cash);
(aa) Complex, unusual or large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose;
(bb) *Business relationships* or *occasional transactions* undertaken through intermediaries such as a *customer*'s adviser;
(cc) Payments made to, or received from, unknown or un-associated third parties;
(dd) The use of cash;
(ee) The use of wire transfers of *funds* allowing quick and complicated movement of substantial *funds* across jurisdictional lines;
(ff) The creation of companies or other types of *legal person* or *legal arrangement* whose purpose and activities are unclear;
(gg) Charitable or political donations and political sponsorship; and
(hh) Transactions relating to advisory and consulting activities with no apparent connection to the known activities of the business;

61. Fraud and tax evasion *risk*:

Fraud is a predicate offence which can incorporate a wide variety of criminal activity. The *NRA* identifies case studies with foreign fraud as the underlying offence, including credit card fraud, securities fraud and frauds relating to Ponzi schemes. Bribery and corruption offences will often be linked to fraud as individuals are obtaining funds fraudulently.

In relation to tax evasion offences in *the Bailiwick*, the *NRA* has identified that the most likely taxes to be evaded are income tax and corporation tax and this applies to individual natural persons and is committed either by individuals, indirectly, directly or through the misuse of trusts and companies, or by corporations. Where corporation tax is evaded, the *Bailiwick*'s experience is that this has involved companies connected to extractive industries and the financial services sector, principally with tax residence in the UK, Europe or the US.

General *risk* factors:

(a) Moving some of a *customer*'s assets out of their legal ownership or out of their home jurisdiction for which there is no clear legitimate rationale or purpose; and
(b) The creation of corporate structures with no legitimate purpose or rationale through which sham loan arrangements are entered into.

Customer risk factors:

(c) Non-resident *customers* with no legitimate reasons for using financial services in another country or jurisdiction;

(d) *Legal persons* or *legal arrangements* that are personal asset holding vehicles where their purpose is unclear and/or beneficial ownership is unclear;
(e) Companies that have *nominee shareholders* whose use is unclear, or shares in bearer form;
(f) Cash intensive businesses; and
(g) The ownership structure of a *legal person* or *legal arrangement* appears unusual or excessively complex with no clear legitimate reasons.

Countries and territories *risk* factors:

(h) Countries identified by credible sources as not having adequate AML/CFT/CPF approaches; and
(i) Countries perceived to have high levels of secrecy or used as a tax shelter, which do not subscribe to international tax exchange standards such as the OECD's Common Reporting Standard.

Product, service, transaction or delivery channel *risk* factors:

(j) Private banking for the reasons in paragraph 3.60(y) above;
(k) Anonymous transactions (which may include cash);
(l) *Business relationships* or *occasional transactions* undertaken through intermediaries such as a *customer*'s adviser;
(m) Payments received from unknown or un-associated third parties;
(n) Complex tax planning structures involving high levels of secrecy;
(o) Overly complex supply chains;
(p) Transactions relating to high value projects;
(q) Transactions involving multiple parties, jurisdictions and/or professional enablers with no clear purpose and rationale; and
(r) Loan arrangements with no clear purpose and rationale.

62. Below are example *risk* factors for other predicate offences, including *terrorist financing* and *proliferation financing*, that may be considered by the firm as part of the assessments of its *ML, TF* and *PF risks*. The examples given are not intended to be exhaustive or to be used by the firm as checklists of *risks*.

Customer risk:

(a) The countries, territories and geographic areas with which *customers* (and the *beneficial owners* of *customers*) have a *relevant connection*;
(b) The complexity of *customer* and beneficial ownership structures;
(c) The complexity of *legal persons* and *legal arrangements*;
(d) The use of introduced business arrangements;
(e) The use or acceptance of *intermediary relationships*;
(f) The number of *business relationships* assessed as high *risk*;
(g) The countries and geographic areas targeted by the firm and from which the firm will accept new *customers* (including the *beneficial owners* of *customers*);
(h) The number of *customers* and *beneficial owners* assessed as *PEPs* and their associated countries or territories; and
(i) The number of *customers* and *beneficial owners* which are charities or non-profit organisations ("NPOs") and their associated countries or geographic areas.

Product/service *risk*:

(j) The nature, scale, diversity and complexity of the products and services of the firm;
(k) The target markets, both in terms of geography and class of *customer*;
(l) The distribution channels utilised by the firm;

(m) Whether the value of transactions is expected to be particularly high;
(n) The nature, scale and countries/geographic areas associated with *funds* sent and received on behalf of *customers*;
(o) Whether payments to any unknown or un-associated third parties are allowed; and
(p) Whether the products/services/structure are of particular, or unusual, complexity.

Other potential sources of *risk* to consider:

(q) Internal and/or external audit findings;
(r) Typologies and findings of *ML, TF* and *PF* case studies;
(s) UNSCR targeted financial sanctions relating to *TF* and *PF*;
(t) UK and *Bailiwick* sanctions; and
(u) Designation of persons under EU, OFAC and other sanctions.

3.11. New Products and Business Practices

63. In accordance with Paragraphs 3(3)(c)(i) and 16A of *Schedule 3*, the firm shall, before making available or adopting new products or business practices, ensure that its *business risk assessments* have identified and assessed the *ML, TF* and *PF risks* arising from those products or practices.

64. References to new products should be read as referring to products which the firm has not previously offered and which present new or differing *ML, TF* or *PF risks* to the firm.

65. References to new business practices relate to new ways in which the firm's products or services are offered or delivered. For example, a new business practice could include the development of a *customer*-facing portal or other software where *customers* can interact with the firm.

66. If the firm decides to proceed with the offering or adoption of a new product or business practice, the *board* of the firm must approve the *risk* assessment undertaken in accordance with Paragraph 3(3)(c)(i) of *Schedule 3* and that approval must be documented.

3.12. New and Developing Technologies

67. In accordance with Paragraph 3(3)(c)(ii) of *Schedule 3*, the firm shall, before adopting and using a new or developing technology for a new or pre-existing product, ensure that its *business risk assessments* have identified and assessed the *risks* arising from the technology's use or adoption.

68. These technologies are likely to fall within the Financial Technology ("FinTech") arena, which includes technology aimed at disrupting the delivery or transaction channels of traditional products and services, as well as the creation of new products or services utilising enhancements in technology. Examples of such technologies include the use of distributed ledger technology in the delivery of traditional securities, the trading or safekeeping of *virtual assets*, through to the use of electronic verification systems to establish the identity of a natural person or use of Artificial Intelligence ("AI"). Risks associated with *virtual assets* are included within Section 18.8 of this *Handbook* to assist all firms who are considering engaging in *virtual asset* activities, as well as *VASP*s.

69. The *risk* assessment of a new or developing technology must include, as a minimum, an assessment of the *ML, TF* and *PF risks* and vulnerabilities inherent in the use or adoption of the technology in order that appropriate controls can be implemented. This includes evaluating the technology itself, together with the anticipated use of the technology and the threats posed by this use, in advance of its deployment.

70. It is not essential that the *risk* assessment of a technology extends to a highly technical, comprehensive report on the specifications and functionality. The objectives of the *risk* assessment are to assist the firm's understanding of the technology it is adopting, to evaluate the *ML, TF* and *PF risk*s which would arise from its use, including any new *risks* to the firm, and the vulnerabilities inherent in the use of the technology in order to identify the controls necessary to mitigate and limit the firm's exposure to those *risks*.

71. For firms which are part of a group which is introducing new technology or developing technology for use within the group, the firm may rely on the group's *ML/TF/PF risk* assessment, provided the assessment considers in sufficient detail the nature of the firm's business and risk profile, which may differ from other parts of the group. The firm should have a copy of the assessment with which its Board or its senior managers are familiar. If the assessment is not sufficient to meet the firm's obligations under Schedule 3 and the *Commission Rules* in this *Handbook*, the firm should conduct its own risk assessment of the technology.

72. It is also important that the firm considers and plans how the technology it is considering adopting will be implemented, particularly where it involves integration with existing systems, as poor implementation can create vulnerabilities in the firm's overall controls for preventing and detecting ML, TF and PF. Implementation plans should cover the following areas:-

    a) ensuring that the firm's AML/CFT/CPF policies, procedures and controls accurately reflect how the technology is to be used and updating them as required;
    b) good data governance around the underlying data to ensure it is accurate, complete, accessible, up to date and relevant;
    c) appropriate user testing and management reporting of results before formal roll-out;
    d) provision of appropriate training to staff who will be using the technology;
    e) provision of appropriate training to staff in compliance roles testing its output as part of the firm's compliance monitoring programme;
    f) ensuring appropriate risk-based systems testing, both before and during deployment of the technology; and
    g) ensuring that the firm makes appropriate investment in the full suite of systems required, including any additional resourcing and system upgrade requirements.

    The Commission's Cyber Security Rules and Guidance may also assist the firm's development of its use of technology.

    Cyber Security Rules and Guidance, 2021.pdf

73. Depending on the nature of the technology being considered, a technology risk assessment should consider the following areas:

    a) the robustness, resilience and security of the technology from the risk of data loss, particularly from cyber-attacks;
    b) how the technology enables the firm to comply with its obligations under *Schedule 3* and this *Handbook*, including for example the regulatory requirements in relation to *CDD*, activity/transaction monitoring, record-keeping and sharing relevant data within the firm, its group (if applicable) and relevant authorities such as the Commission and the FIU, as relevant to the technology being considered;
    c) where the technology leads to faster transaction times, the ability of the firm to monitor and intervene in an unusual transaction which may give rise to a suspicion of ML, TF or PF; and
    d) any supplier related issues which could impact its operation.

    A firm considering adopting electronic verification systems should ensure its assessment covers areas set out in *Commission Rules 5.28*, 5.34 and guidance in paragraph 5.35 of the *Handbook*.

74. If the firm decides to proceed with the adoption or use of a new or developing technology for a new or pre-existing product, the *board* of the firm must approve the *risk* assessment undertaken in accordance with Paragraph 3(3)(c)(ii) of *Schedule 3* and that approval must be documented.

75. Following the initial *risk* assessment of a new or developing technology, the firm should periodically review its assessment in conjunction with its responsibility for the review of its wider *ML, TF* and *PF business risk assessments* as described in Section 3.9. of this *Handbook*, particularly in light of the fast pace of technological developments.

Relationship Risk Assessment

3.13. Introduction

76. The purpose of this Section is to set out the *Commission Rules* and *guidance* surrounding the assessment of *risk* in a *business relationship* or *occasional transaction* ("*relationship risk assessment*") at the point of take-on, as well as the ongoing requirement to ensure that any *relationship risk assessment* remains appropriate and relevant as the relationship evolves.

77. The firm's *business risk assessments* and its defined *risk appetite* will assist in determining the take-on of any new business. The *relationship risk assessment* is the assessment of a new or existing *business relationship* or *occasional transaction* against the parameters determined within the *risk appetite* and the *ML, TF* and *PF risks* identified in the *business risk assessments*.

78. There may be circumstances where the *risks* of *ML, TF* and *PF* are high and *ECDD* measures are to be applied. Similarly, there may be circumstances within which the firm can apply *SCDD* measures because it has assessed the *risk* of the *business relationship* or *occasional transaction* as being low. Further information on the *relationship risk assessment* process, including examples of high and low *risk* factors, can be found in this Section.

3.14. Management and Mitigation

79. In order to consider the extent of its potential exposure to the *risk*s of *ML, TF* and *PF*, in accordance with Paragraph 3(4) of *Schedule 3* the firm shall -

    (a) prior to the establishment of a *business relationship* or the carrying out of an *occasional transaction*, undertake a *relationship risk assessment*, and
    (b) regularly review any *relationship risk assessment* carried out under (a) so as to keep it up to date and, where changes to that *relationship risk assessment* are required, it shall make those changes.

80. Based on the outcome of its *relationship risk assessment*, the firm must decide whether or not to accept (or continue) each *business relationship* or whether or not to accept any instructions to carry out an *occasional transaction*.

81. When undertaking or reviewing a *relationship risk assessment*, in accordance with Paragraph 3(5)(a) of *Schedule 3* the firm shall take into account its *risk appetite* and *risk* factors relating to:

    (i) the type or types of *customer* (and the *beneficial owners* of the *customer*);
    (ii) the country or geographic area; and
    (iii) the product, service, transaction and delivery channel that are relevant to the *business relationship* or *occasional transaction.*

82. The FATF publishes two lists identifying jurisdictions with weak measures to combat *ML, TF* and *PF*. The first list is of "High risk jurisdictions subject to a call for action" which identifies a

number of countries and territories with significant strategic deficiencies in their regimes to counter *ML*, *TF* and *PF*. Appendix H to this *Handbook* identifies those countries and territories which the FATF has listed as high *risk* and has called on jurisdictions to apply enhanced due diligence. In the most serious cases, it will also call upon jurisdictions to apply counter-measures to protect the international financial system from the ongoing *ML*, *TF* and *PF* risks emanating from that country.

83. The second list issued by the FATF is a statement of those "jurisdictions under increased monitoring". These jurisdictions are actively working with the FATF to address strategic deficiencies in their AML/CFT/CPF regimes. The FATF does not call for the application of enhanced due diligence measures to be applied to these jurisdictions, but encourages members to take into account the information it publishes about these jurisdictions in their *risk* analysis. These jurisdictions will be communicated to firms by way of updates to Appendix I, which lists these countries. Appendix I also lists countries and territories that are identified by the UK, US governments, intergovernmental and supranational organisations as presenting certain *ML* and *TF risks*. Alongside these sources, information is presented reflecting assessments of a country or territory by non-governmental organisations which firms may also find useful when they are determining the level of country *risk* presented by a *business relationship* or *occasional transaction*. The inclusion of a country or territory in Appendix I does not automatically imply that a *business relationship* or *occasional transaction* with a *relevant connection* to a country or territory on Appendix I is high *risk.*

84. For the purposes of Paragraph 3(5)(a) of *Schedule 3,* when considering country or geographical area *risk* factors, the firm should:

(a) take into account the information set out in Appendix H to this *Handbook* when undertaking or reviewing a *relationship risk assessment*, as the firm shall apply *ECDD* measures to a *business relationship* or *occasional transaction* where the *customer* or *beneficial owner* has a *relevant connection* with a country or territory in Appendix H;
(b) consider the specific *ML* and *TF risks* of the countries and territories listed in Appendix I and how those *risks* affect the overall *risk* within a *business relationship* or *occasional transaction* as set out in Section 3.4. of this *Handbook*; and
(c) consider the relevance of the *risk* factors in Section 3.17.2. of this *Handbook*.

85. In addition to the *risk* factors set out above, the firm must also give consideration to the following when undertaking or reviewing a *relationship risk assessment*:

(a) where the product or service provided by the firm is a life insurance policy, the type or types of beneficiary of that policy;
(b) the purpose and intended nature of the *business relationship* or *occasional transaction*, including the possibility of *legal persons* and *legal arrangements* forming part of the relationship;
(c) the type, volume, value and regularity of activity expected; and
(d) the expected duration (if a *business relationship*).

86. For the purposes of Paragraph 3(5)(a) of *Schedule 3* and *Commission Rule* 3.85.(a) above, the firm's consideration of the type or types of *customer*, *beneficial owner* or beneficiary should incorporate whether they are a natural person, *legal person* or *legal arrangement*, as well as their identity and background.

87. In accordance with Paragraph 3(5)(b) of *Schedule 3*, when undertaking or reviewing a *relationship risk assessment*, the firm shall understand that the *risk* factors noted in Paragraph 3(5)(a) of *Schedule 3* as set out above and any other *risk* factors, either singly or in combination, may increase or decrease the potential *risk* posed by the *business relationship* or *occasional transaction*.

88. In light of the above, when undertaking a *relationship risk assessment* the firm must ensure that all relevant *risk* factors are considered, both singly and in combination, before making a determination as to the level of overall assessed *risk*.

89. Consideration of the purpose and intended nature of a *business relationship* or *occasional transaction* in accordance with *Commission Rule* 3.85.(b) should include an assessment of the economic or other commercial rationale for the *business relationship* or *occasional transaction*.

90. The firm's procedures may provide for standardised profiles to be used for *relationship risk assessments* where the firm has *satisfied* itself, on reasonable grounds, that such an approach effectively manages the *risk* for each particular *business relationship* or *occasional transaction*. However, where the firm has a diverse *customer* base, or where a wide range of products and services are offered, it must develop a more structured and rigorous system to show that judgement has been exercised on an individual basis rather than on a generic or categorised basis.

91. Whatever method is used to assess the *risk* of a *business relationship* or *occasional transaction*, the firm must maintain clear documented evidence as to the basis on which the *relationship risk assessment* has been made.

92. Where, despite there being high *risk* factors identified, the firm does not assess the overall *risk* as high because of strong and compelling mitigating factors, the firm must identify the mitigating factors and, along with the reasons for the decision, *document* them and retain them on the relevant *business relationship* or *occasional transaction* file.

93. Based upon the results of the *relationship risk assessment*, the firm must determine, on the basis of *risk*:

    (a) the extent of the identification information to be obtained on the *key principals* to the *business relationship* or *occasional transaction* in accordance with Paragraphs 4 and 5 of *Schedule 3* and Chapters 4 to 8 of this *Handbook*;
    (b) how and to what extent that information will be verified using *identification data*;
    (c) whether to apply *SCDD* measures where the *business relationship* or *occasional transaction* has been assessed as being low *risk* and displays one or more of the characteristics in Chapter 9 of this *Handbook*; and
    (d) the extent to which the resulting *business relationship* will be monitored on an ongoing basis.

94. The *relationship risk assessment* is to be carried out prior to the establishment of a *business relationship* or the carrying out of an *occasional transaction*. However, given that *risk* is dynamic, it is important that, in the case of an existing *business relationship*, the *relationship risk assessment* be reviewed from time to time, the frequency of which will depend on the level of *risk* presented by the particular *business relationship*. It is also especially important where there is a trigger event marking a material departure from the business and *risk* profile of the *customer* which may be noted through the ongoing monitoring of transactions and activity (e.g., a *customer* acquires a new service or product or is subject to some form of adverse media). Moreover, a revision of a *customer's relationship risk assessment* may also be required when the firm identifies new *risk* factors and amends its *business risk assessments*.

3.15. Notices, Instructions or Warnings

95. From time to time *the Commission* issues Notices, Instructions or Warnings which highlight potential *risks*. This information, together with sanctions legislation applicable in *the Bailiwick*, must be considered when undertaking or reviewing a *relationship risk assessment*.

96. It is unlawful to engage in proliferation financing in *the Bailiwick.* Guidance on combatting proliferation and proliferation financing has been issued by the Policy and Resources Committee and can be found through the following link:

https://www.gov.gg/wmd

Further information on *the Bailiwick's* sanctions regime and legislation can be found in Chapter 12 of this *Handbook.*

3.16. Mandatory High Risk Factors

97. In accordance with Paragraph 5(1) of *Schedule 3*, where the firm is required to carry out *CDD* measures, it must also carry out *ECDD* measures in relation to high *risk business relationships* and *occasional transactions,* including, without limitation -

(a) a *business relationship* or *occasional transaction* in which the *customer* or any *beneficial owner* is a *foreign PEP*;
(b) where the firm is an *FSB*, a *business relationship* which is –

(i) a *correspondent banking relationship*, or
(ii) similar to such a relationship in that it involves the provision of services, which themselves amount to *financial services business* or facilitate the carrying on of such business, by one *FSB* to another;

(c) a *business relationship* or an *occasional transaction* –

(i) where the *customer* or *beneficial owner* has a *relevant connection* with a country or territory that -

(A) provides funding or support for terrorist activities, or does not apply (or insufficiently applies) *the FATF Recommendations*, or
(B) is a country otherwise identified by the FATF as a country for which such measures are appropriate,

(ii) which the firm considers to be a *high risk relationship*, taking into account any notices, instructions or warnings issued from time to time by *the Commission* and having regard to the *NRA,*

(d) a *business relationship* or an *occasional transaction* which has been assessed as a *high risk relationship*, and
(e) a *business relationship* or an *occasional transaction* in which the *customer*, the *beneficial owner* of the *customer*, or any other *legal person* in the ownership or control structure of the *customer*, is a *legal person* that has *bearer shares* or *bearer warrants*.

98. Chapter 8 of this *Handbook* sets out the requirements of *Schedule 3* and the *Commission Rules* in relation to *high risk relationships* and includes details of sources which may assist in the assessment of *risk.*

99. The firm is required to have regard to the *NRA* in determining what constitutes a high or low *risk*, what its *risk appetite* is, and what constitutes appropriate measures to manage and mitigate *risks*. The sections of the *NRA* which discuss the modalities of *ML, TF* and *PF*, and the case studies contained within, are particularly relevant to the firm when assessing and mitigating *customer*, product, service, transaction and delivery channel *risk* factors.

3.17. Risk Factors

100. The *risk* factors included within the following sections are purely for guidance and are provided as examples of factors that the firm might consider when undertaking a *relationship risk assessment*. The following factors are not exhaustive and are not prescribed as a checklist. It is for the firm to assess and decide what is appropriate in the circumstances of the *business relationship* or *occasional transaction* and it is not expected that all factors will be considered in all cases.

101. The example indicators do not remove the ability of the firm to apply a *risk*-based approach. In this respect the firm should take a holistic view of the *risk* associated with each *business relationship* or *occasional transaction* as set out in Section 3.4. of this Chapter. The presence of isolated *risk* factors does not necessarily move a *business relationship* or *occasional transaction* into a higher or lower *risk* category; however, in accordance with Section 3.4.1. above, certain *risk* factors could have a bigger contribution to the overall *risk* assessment than others.

102. If it is determined, through a *relationship risk assessment*, that there are types of *customer*, activity, business or profession that are at *risk* of abuse from *ML*, *TF* and/or *PF*, then the firm should apply higher AML/CFT/CPF requirements as dictated by the relevant *risk* factor(s).

3.17.1. Customer Risk Factors

103. When identifying the *risk* associated with its *customers*, including the *beneficial owners* of *customers*, the firm should consider the *risk* related to:

(a) the *customer's* (and *beneficial owner's)* business or professional activity;
(b) the *customer's* (and *beneficial owner's*) reputation; and
(c) the *customer's* (and *beneficial owner's*) nature and behaviour.

104. *Risk* factors that may be relevant when considering the *risk* associated with a *customer's* or *beneficial owner's* business or professional activity include:

(a) Does the *customer* or *beneficial owner* have links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the arms trade and defence, the extractive industries, public procurement or energy industries?
(b) Does the *customer* or *beneficial owner* have links to sectors that are associated with higher *ML, TF* and/or *PF risk*, for example, certain money service providers ("MSPs"), casinos, dealers in precious metals or trading companies?
(c) Does the *customer* or *beneficial owner* have links to sectors that involve significant amounts of cash?
(d) Where the *customer* is a *legal person* or *legal arrangement*, what is the purpose of their establishment? For example, what is the nature of their business?
(e) Does the *customer* have political connections, for example, are they a *PEP*, or is the *beneficial owner* a *PEP*? Does the *customer* or *beneficial owner* have any other relevant links to a *PEP*, for example, are any of the *customer's* directors *PEPs* and, if so, do these *PEPs* exercise significant control over the *customer* or *beneficial owner*? In line with Paragraph 5(1) of *Schedule 3*, where a *customer* or the *beneficial owner* is a *foreign PEP* the firm shall apply *ECDD* measures.
(f) Does the *customer* or *beneficial owner* hold another prominent position or enjoy a high public profile that might enable them to abuse this position for private gain? For example, are they senior local or regional public officials with the ability to influence the awarding of public contracts, decision-making members of high-profile sporting bodies or individuals who are known to influence the government and other senior decision-makers?
(g) Is the *customer* a *legal person* subject to enforceable disclosure requirements that ensure reliable information about the *customer's beneficial owner* is publicly available, for

example, public companies listed on stock exchanges that make such disclosure a condition for listing?

(h) Is the *customer* an *FSB* acting on its own *account* from a country or territory listed in Appendix C to this *Handbook*? Is there evidence that the *customer* has been subject to supervisory sanctions or enforcement for failure to comply with AML/CFT/CPF obligations or wider conduct requirements in recent years?

(i) Is the *customer* a public administration or enterprise from a country or territory with low levels of corruption?

(j) Is the *customer's* or the *beneficial owner's* background consistent with what the firm knows about their former, current or planned business activity, their business's turnover, the source of *funds* and the *customer's* or *beneficial owner's* source of wealth?

(k) Is the *customer* a money remitter in a higher *risk* jurisdiction for terrorism or *terrorist financing* whose activities could be abused for *TF* purposes?

(l) Is the customer a Non-Profit Organisation ("NPO") whose activities could be abused for *TF* purposes, in particular those NPOs operating directly or indirectly in higher *risk* jurisdictions for terrorism?

(m) Is the *customer* a legal person involved in the trade of dual use goods (goods that have legitimate commercial or industrial uses, and may also be used in WMD) which could be used for *PF* purposes directly or indirectly by the Democratic People's Republic of Korea or Iran?

(n) Is the *customer* involved in business with or have a relevant connection to a country of diversion concern or *PF* hub jurisdiction as referred to in section 8.40 of the *NRA* and Figure 4 and Annex A of the *PF* Guidance issued by the States of Guernsey Policy & Resources Committee?

105. The following *risk* factors may be relevant when considering the *risk* associated with a *customer's* or *beneficial owner's* reputation:

(a) Are there adverse media reports or other relevant sources of information about the *customer*, for example, are there any allegations of criminality, *terrorism* or *proliferation financing* against the *customer* or the *beneficial owner*? If so, are these reliable and credible? The firm should determine the credibility of allegations on the basis of the quality and independence of the source of the data and the persistence of reporting of these allegations, among other considerations. The firm should note that the absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing.

(b) Has the *customer*, *beneficial owner* or anyone publicly known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism, *TF* or *PF*? Does the firm have reasonable grounds to suspect that the *customer* or *beneficial owner* or anyone publicly known to be closely associated with them has, at some point in the past, been subject to such an asset freeze or PF sanctions?

(c) Are there adverse reports or other relevant sources indicating that the *customer*, or *beneficial owner* (or anyone publicly known to be closely associated with them) supports or promotes violent extremism or terrorism?

(d) Does the firm know if the *customer* or *beneficial owner* has been the subject of an internal or external disclosure in the past?

(e) Does the firm have any in-house information about the *customer's* or the *beneficial owner's* integrity, obtained, for example, in the course of a long-standing *business relationship*?

106. The following *risk* factors may be relevant when considering the *risk* associated with a *customer's* or *beneficial owner's* nature and behaviour. The firm should note that not all of these *risk* factors will be apparent at the outset, they may emerge only once a *business relationship* has been established:

(a) Does the *customer* have legitimate reasons for being unable to provide robust evidence of their identity, for example, because they are an asylum seeker?
(b) Does the firm have any doubts about the veracity or accuracy of the *customer's* or *beneficial owner's* identity?
(c) Are there indications that the *customer* might seek to avoid the establishment of a *business relationship*? For example, does the *customer* look to carry out one transaction or several one-off transactions where the establishment of a *business relationship* might make more economic sense?
(d) Is the *customer's* ownership and control structure transparent and does it make sense? If the *customer's* ownership and control structure is complex or opaque, is there an obvious commercial or lawful rationale?
(e) Does the *customer* issue *bearer shares* or does it have *nominee shareholders*?
(f) Is the *customer* a *legal person* or *legal arrangement* that could be used as a personal asset holding vehicle?
(g) Is there a sound reason for changes in the *customer's* ownership and control structure?
(h) Does the *customer* request transactions that are complex, unusual or unexpectedly large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale? Are there grounds to suspect that the *customer* is trying to evade specific thresholds, such as those subject to mandatory reporting, either in *the Bailiwick* or the *customer's* home country or territory?
(i) Does the *customer* request unnecessary or unreasonable levels of secrecy? For example, is the *customer* reluctant to share *identification data*, or do they appear to want to disguise the true nature of their business?
(j) Can the *customer's* or *beneficial owner's* source of *funds* or source of wealth be easily established, for example, through their occupation, inheritance or investments?
(k) Does the *customer* use the products and services they have taken out as expected when the *business relationship* was first established?
(l) Has the *customer* made unexpected financial donations to NPOs whose activities could be abused for *TF* purposes, in particular those NPOs operating directly or indirectly in higher *risk* jurisdictions for terrorism?
(m) Does the *customer* make use of crowdfunding or social media platforms to move small amounts of money?

3.17.2. Countries and Territories Risk Factors

107. Internationally, it is recognised that *ML* often involves using the financial systems of a number of jurisdictions. Analysis was undertaken as part of the *NRA* as to how *the Bailiwick* typically fits into this pattern. The findings from this analysis were that in the majority of cases *the Bailiwick's* involvement is distant from or peripheral to the criminal enterprises. This indicates in turn that in most cases involving foreign criminal proceeds, *the Bailiwick* is likely to be some way removed from the criminality itself and to come a considerable distance down the chain of laundering activity, therefore, the firm should consider country *risk* in the round, where *risks* are higher ensuring it fully understands the source of those *funds*.

108. When identifying the *risk* associated with countries and territories, the firm should consider the *risk* related to those countries and territories with which the *customer* or *beneficial owner* has a *relevant connection*.

109. The firm should note that the nature and purpose of the *business relationship* will often determine the relative importance of individual country and geographical *risk* factors. For example:

(a) Where the *funds* used in the *business relationship* or *occasional transaction* have been generated abroad, the level of predicate offences to *ML* and the effectiveness of a country's or territory's legal system will be particularly relevant.

(b) Where *funds* are received from, or sent to, countries or territories where groups committing terrorist offences are known to be operating, the firm should consider to what extent this could be expected to, or might give rise to, suspicion based on what the firm knows about the purpose and nature of the *business relationship* or *occasional transaction*.
(c) Where the *customer* is an *FSB*, the firm should pay particular attention to the adequacy of the country's or territory's AML/CFT/CPF regime and the effectiveness of AML/CFT/CPF supervision.
(d) Where the *customer* or *beneficial owner* is a *legal person* or *legal arrangement*, the firm should take into account the extent to which the country or territory in which the *customer* or *beneficial owner* is registered effectively complies with international tax transparency standards.

110. *Risk* factors the firm should consider when identifying the effectiveness of a country's or territory's AML/CFT/CPF regime include:

(a) Has the country or territory been identified by a mutual evaluation as having strategic deficiencies in its AML/CFT/CPF regime? In accordance with Paragraph 5(1)(c)(i) of *Schedule 3*, *ECDD* measures shall be applied where the *customer* or *beneficial owner* has a *relevant connection* to a country or territory that does not apply (or insufficiently applies) *the FATF Recommendations*. Further information can be found in Section 3.15. of this Chapter.
(b) Is there information from more than one credible and reliable source about the quality of the country's or territory's AML/CFT/CPF controls, including information about the quality and effectiveness of regulatory enforcement and oversight? Examples of possible sources include mutual evaluation reports by the FATF or FATF-style regional bodies (in particular Recommendations 10, 26 and 27 and Immediate Outcomes 3 and 4), the FATF's list of high-risk and non-cooperative jurisdictions, International Monetary Fund ("IMF") assessments and Financial Sector Assessment Programme reports. The firm should note that membership of the FATF or a FATF-style regional body (for example, MONEYVAL) does not, of itself, mean that the country's or territory's AML/CFT/CPF regime is adequate and effective.
(c) Information in Appendices H and I to this *Handbook*, which list a number of countries and territories that are identified by relevant and external sources as presenting a higher *risk* of *ML*, *TF* and *PF*.

111. *Risk* factors the firm should consider when identifying the *risk* associated with the level of predicate offences to *ML* in a country or territory include:

(a) Is there information from credible and reliable public sources about the level of other predicate offences to *ML* in the country or territory, such as, but not limited to, insider trading and/or market manipulation, drug trafficking, cybercrime, environmental crime, human trafficking or wildlife trafficking?
(b) Is there information from one or more credible and reliable sources about the capacity of the country's or territory's investigative and judicial system to effectively investigate and prosecute these offences?

112. *Risk* factors the firm should consider when identifying the level of *TF* and *PF risk* associated with a country or territory include:

(a) Is there information (for example, from law enforcement or credible and reliable open media sources) suggesting that a country or territory provides funding or support for terrorist activities or organisations within that country or territory?
(b) Is there information (for example, from law enforcement or credible and reliable open media sources) suggesting that groups committing terrorist offences are known to be operating in the country or territory?

(c) Is the country or territory subject to financial sanctions, embargoes or measures that are related to terrorism, *TF* or *PF* issued by, the UN, UK and/or *Bailiwick* sanctions?
(d) Are there communities within the country or territory that may be actively targeted by terrorist organisations for support or cover or who may be sympathetic to terrorist actors because of diaspora links or other connections?
(e) Is the country or territory rich in natural/environmental resources and is known to have active terrorist organisations operating within it?
(f) Is the country or territory a regional or international financial centre in close proximity to a conflict zone or to a country or territory identified as funding or supporting terrorist activities which could increase the risk of that finance centre being used as a transit jurisdiction to move *funds* linked with terrorist activity?
(g) Is *TF* criminalised or inadequately criminalised in the country or territory? Information on this may be found in its FATF or equivalent mutual evaluation report.

113. *Risk* factors the firm should consider when identifying a country's or territory's level of transparency and tax compliance include:

(a) Is there information from more than one credible and reliable source that the country has been deemed compliant with international tax transparency and information sharing standards? Is there evidence that relevant rules are effectively implemented in practice? Examples of possible sources include reports by the Global Forum on Transparency and the Exchange of Information for Tax Purposes of the OECD, which rate jurisdictions for tax transparency and information sharing purposes; assessments of the country's or territory's commitment to automatic exchange of information based on the Common Reporting Standard; assessments of compliance with Recommendations 9, 24 and 25 and Immediate Outcomes 2 and 5 of *the FATF Recommendations* by the FATF or FATF-style regional bodies; and IMF assessments (for example, IMF staff assessments of offshore financial centres).
(b) Has the country or territory committed to, and effectively implemented, the Common Reporting Standard on Automatic Exchange of Information, which the G20 adopted in 2014?
(c) Has the country or territory put in place reliable and accessible beneficial ownership registers?

114. *Risk* factors the firm should consider when identifying the *risk* associated with the level of bribery and corruption associated with a country or territory include:

(a) Is there information from credible and reliable public sources about the level of bribery and corruption associated with a country or territory? Examples include OECD country reports on the implementation of the OECD's anti-bribery convention, corruption perceptions indices, Organization of American States' Inter American Convention against Corruption (IACAC), the Mechanism for Follow-Up on the Implementation of the IACAC (MESICIC) and the Council of Europe's Group of States Against Corruption (GRECO). Consideration should also be given regarding whether a peer assessment of an individual country's progress on implementing international standards to address bribery and corruption is available.
(b) For higher risk countries or territories are public officials and political persons required to disclose their assets and business interests by law?
(c) Does the country or territory require disclosure and transparency of public contracts?
(d) Does the country or territory comply sufficiently with *the FATF Recommendations* (information is available in their mutual evaluation reports)?
(e) Are there relevant reports and databases on corruption *risk* available that have been published by specialised national, international, non-governmental and commercial organisations? The IMF, World Bank (the Worldwide Governance Indicators project) and

some non-governmental organisations, including Transparency International, publish relevant reports or compile indices measuring corruption.

(f) Are the country or territory's companies reported to engage in bribery when doing business abroad, for example, by having poor ratings in Transparency International's Bribe Payers Index?

(g) Has the country or territory ratified and implemented the provisions of the United Nations Convention against Corruption (UNCAC)? Ratification of these provisions evidences a nation's willingness to combat corruption, but does not evidence that the provisions have been implemented.

(h) Is there information from more than one credible and reliable source about the capacity of the country or territory's investigative and judicial system to effectively investigate and prosecute bribery and corruption offences?

3.17.3. Products, Services and Transactions Risk Factors

115. When identifying the *risk* associated with its products, services or transactions, the firm should consider the *risk* related to:

(a) the level of transparency, or opaqueness, the product, service or transaction affords;
(b) the complexity of the product, service or transaction; and
(c) the value or size of the product, service or transaction.

116. *Risk* factors that may be relevant when considering the *risk* associated with a product, service or transaction's transparency include:

(a) To what extent do products or services allow the *customer* or *beneficial owner* structures to remain anonymous, or facilitate hiding their identity? Examples of such products and services include *bearer shares*, fiduciary deposits, personal asset holding vehicles, and legal entities such as *foundations* that can be structured in such a way as to take advantage of anonymity and allow dealings with shell companies or companies with *nominee shareholders*.

(b) To what extent is it possible for a third party that is not part of the *business relationship* to give instructions, for example, in the case of certain *correspondent banking relationships*?

(c) To what extent could the products or services have been stolen by persons acting for a country who is subject to *PF* sanctions? For example, the use of *virtual assets* by Iran and the Democratic People's Republic of Korea and the hacking of such assets by these countries subject to *PF* sanctions.

117. *Risk* factors that may be relevant when considering the *risk* associated with a product, service or transaction's complexity include:

(a) To what extent is the transaction complex and does it involve multiple parties or multiple countries or territories, for example, in the case of certain trade finance transactions? Are transactions straightforward, for example, are regular payments made into a pension fund?

(b) To what extent do products or services allow payments from third parties or accept overpayments where this would not normally be expected? Where third party payments are expected, does the firm know the third party's identity, for example, is it a state benefit authority or a guarantor? Or are products and services funded exclusively by *fund* transfers from the *customer's* own *account* at another *FSB* that is subject to AML/CFT/CPF standards and oversight that are comparable to those in *the Bailiwick*?

(c) Does the firm understand the *risks* associated with its new or innovative product or service, in particular where this involves the use of new technologies or payment methods?

118. *Risk* factors that may be relevant when considering the *risk* associated with a product, service or transaction's value or size include:

(a) To what extent are products or services cash intensive, for example, many payment services and certain current *accounts*?
(b) To what extent do products or services facilitate or encourage high-value transactions? Are there any caps on transaction values or levels of premium that could limit the use of the product or service for *ML*, *TF* and *PF* purposes?

3.17.4. Delivery Channel Risk Factors

119. When identifying the *risk* associated with the way in which the *customer* obtains the products or services they require, the firm should consider the *risk* related to:

(a) the extent to which the *business relationship* is conducted on a non-face-to-face basis; and
(b) any introducers of business or other intermediaries the firm might use and the nature of their relationship with the firm.

120. When assessing the *risk* associated with the way in which the *customer* obtains the products or services, the firm should consider a number of factors including:

(a) Is the *customer* physically present for identification purposes? If they are not, has the firm used a reliable form of *identification data*? Has it taken steps to prevent impersonation or identity fraud?
(b) Has the *customer* been introduced by another part of the same financial group and, if so, to what extent can the firm rely on this introduction as reassurance that the *customer* will not expose the firm to excessive *ML*, *TF* or *PF risk*? What has the firm done to satisfy itself that the group entity applies *CDD* measures equivalent to those of the firm?
(c) Has the *customer* been introduced by a third party (for example, an *FSB* that is not part of the same group)? What has the firm done to be *satisfied* that:

    (i) the third party applies *CDD* measures and keeps records to a standard equivalent to *the FATF Recommendations*;
    (ii) the third party will provide, immediately upon request, relevant copies of *identification data* in accordance with Paragraph 10 of *Schedule 3* and Chapter 10 of this *Handbook*; and
    (iii) the quality of the third party's *CDD* measures is such that it can be relied upon?

(d) Has the *customer* been introduced through a tied agent, that is, without direct firm contact? To what extent can the firm be *satisfied* that the agent has obtained enough information so that the firm knows its *customer* and the level of *risk* associated with the *business relationship*?
(e) If independent or tied agents are used, to what extent are they involved on an ongoing basis in the conduct of business? How does this affect the firm's knowledge of the *customer* and ongoing *risk* management?
(f) Where a firm uses an *intermediary*, are there any indications that the *intermediary's* level of compliance with applicable AML/CFT/CPF legislation or regulation is inadequate, for example, has the *intermediary* been sanctioned for breaches of AML/CFT/CPF obligations?

Chapter 4
Customer Due Diligence

Contents of this Chapter

4.1. Introduction

1. The application of *CDD* measures to *business relationships* and *occasional transactions* is important for two key reasons:

   (a) to help the firm, at the time that *CDD* measures are applied, to be *satisfied* that *customers* (and the *beneficial owners* of *customers*) are who they say they are; to know whether the *customer* is acting on behalf of another; and that there is no legal barrier (for example, government sanctions) to providing them with the product or service requested; and
   (b) to enable the firm to assist law enforcement, by providing available information on *customers*, *beneficial owners* or activities being investigated.

2. This Chapter sets out the *Commission Rules* and provides *guidance* in respect of the *CDD* measures to be applied to *business relationships* and *occasional transactions*, including details of the policies, procedures and controls required by the firm in order to meet the relevant requirements of *Schedule 3* and this *Handbook*.

3. The content of this Chapter should be read in conjunction with the following three Chapters: 5. Natural Persons; 6. Certification; and 7. Legal Persons and Legal Arrangements. These Chapters specify the *CDD* measures to be applied based upon the type of *customer* (or *beneficial owner*) with which the firm is entering into a *business relationship* or undertaking an *occasional transaction*.

4. Reference should also be made to Chapters 8. Enhanced Customer Due Diligence and 9. Simplified Customer Due Diligence which provide details of the *ECDD* measures to be applied to *high risk relationships* and the *enhanced measures* for those with specific higher *risk* factors, together with the circumstances in which the firm can apply *SCDD* measures and the details of such measures.

4.2. Overriding Obligations

5. In accordance with Paragraphs 4(2) and 16A of *Schedule 3*, the firm shall apply *CDD* measures when:

   (a) establishing a *business relationship*,
   (b) carrying out an *occasional transaction*,
   (c) the firm knows or suspects or has reasonable grounds for knowing or suspecting –

      (i) that, notwithstanding any exemptions or thresholds pursuant to *Schedule 3*, any party to a *business relationship* is engaged in *ML, TF* or *PF*, or
      (ii) that it is carrying out a transaction on behalf of a person, including a *beneficial owner*, who is engaged in *ML, TF* or *PF*, and

   (d) the firm has doubts about the veracity or adequacy of previously obtained *identification data*.

6. In accordance with Paragraphs 4(5) and 16A of *Schedule 3*, where the firm:

   (a) forms a suspicion of *ML, TF* or *PF* by a *customer* or other person, and
   (b) reasonably believes that carrying out the steps in Paragraphs 4(3), 5(3) or 11 of *Schedule 3* would tip off that *customer* or person,

   it shall not carry out those steps, but shall instead make a disclosure pursuant to Part I of *the Disclosure Law*, or Section 15 or 15A, or Section 12 (as appropriate) of *the Terrorism Law*.

7. Where the firm is a *PSP*, it is also required to apply *CDD* measures when carrying out *occasional transactions* which are *wire transfers* in the circumstances detailed in Chapter 14 of this *Handbook*.

8. Where the firm is a *VASP*, or is a specified business with a connection to, or involvement with, virtual assets, it is also required to apply *CDD* measures and, where relevant, *enhanced measures* and *ECDD* to *business relationships* and *occasional transactions*. Additional rules and guidance relating to *virtual assets* are detailed in Chapter 18 of this *Handbook*.

9. In accordance with Paragraphs 8(1) and 8(2) of *Schedule 3*, in relation to all *customers* the firm shall:

   (a) not set up or keep anonymous *accounts* or *accounts* in fictitious names;
   (b) maintain *accounts* in a manner which facilitates the meeting of the requirements of *Schedule 3* and the relevant *Commission Rules* and *guidance* in this *Handbook*;
   (c) not enter into, or continue, a *correspondent banking relationship* with a *shell bank*; and
   (d) take appropriate measures to ensure that it does not enter into, or continue, a *correspondent banking relationship* where the respondent *bank* is known to permit its *accounts* to be used by a *shell bank*.

10. Sound *CDD* policies and procedures are a key component of an effective AML, CFT and CPF framework and are vital for the firm because they:

    (a) constitute an essential part of *risk* management, providing the basis for identifying, assessing, mitigating and managing *risk*;
    (b) help to protect the firm and the integrity of *the Bailiwick* by reducing the likelihood of the firm becoming a vehicle for, or a victim of, *ML, TF* and/or *PF*;
    (c) help the firm, at the time *CDD* is carried out, to take comfort that the *customer* and other parties included in a *business relationship* or *occasional transaction* are who they say they are and that it is appropriate to provide them with the product or service requested; and
    (d) help the firm to identify, during the course of a continuing *business relationship*, factors which are unusual and which may lead to knowing or suspecting or having reasonable grounds for knowing or suspecting that the parties involved in a *business relationship* or *occasional transaction* may be carrying out *ML, TF* or *PF*.

11. Accordingly, *CDD* is an on-going and cumulative process, the extent of which is determined by both the *risk* attributed to, and the particular circumstances of, a *business relationship* or *occasional transaction*.

4.3. Key Principals

12. Paragraph 4(3) of *Schedule 3* defines the four categories of party which may be associated with a *business relationship* or *occasional transaction* (collectively referred to in the *Handbook* as "*key principals*") and sets out the extent of the *CDD* measures that are to be applied to each of them, specifically:

    (a) the *customer*;
    (b) any person purporting to act on behalf of the *customer*;
    (c) the *beneficial owner* of the *customer*; and
    (d) any person on behalf of whom the *customer* is acting.

4.3.1. The Customer

13. In accordance with Paragraph 4(3)(a) of *Schedule 3*, the *customer* shall be identified and the identity of the *customer* verified using *identification data*.

14. Chapters 5 and 7 of this *Handbook* provide for the *CDD* measures to be applied where the *customer* is a natural person, or a *legal person* and *legal arrangement* respectively.

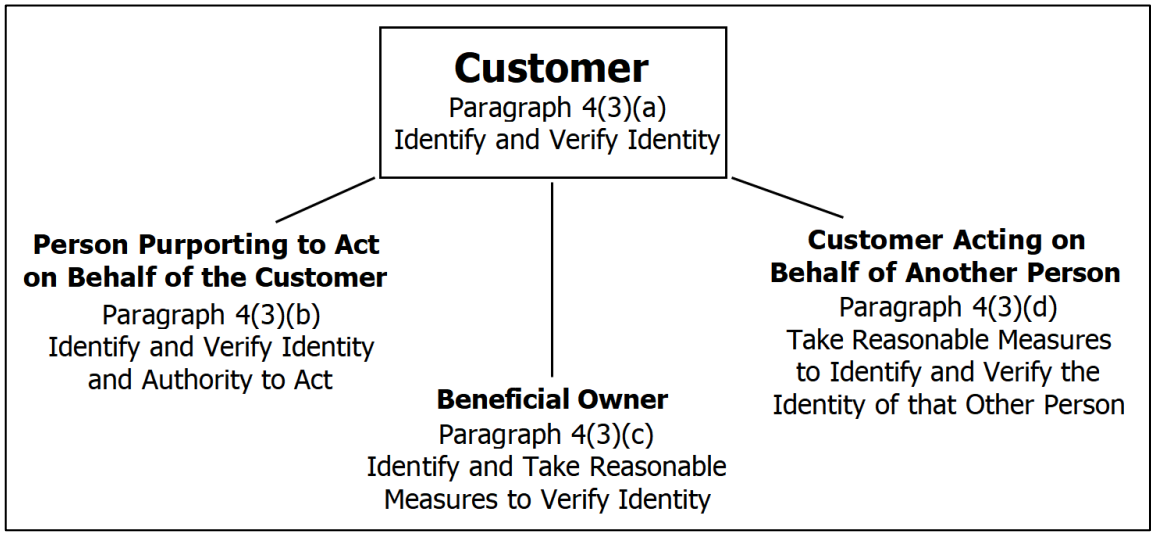


Fig. 1 – CDD Measures for Key Principals

4.3.2. A Person Purporting to Act on Behalf of the Customer

15. In accordance with Paragraph 4(3)(b) of *Schedule 3*, any person purporting to act on behalf of the *customer* shall be identified and that person's identity and authority to so act shall be verified.

16. Examples of such persons will include a guardian of a natural person, the authorised signatories (or equivalent) acting for or on behalf of a *legal person* or *legal arrangement*, those to whom powers of attorney have been granted, the directors (or equivalent) who are acting on behalf of a *legal person*, and any other person acting on behalf of the *customer* within a *business relationship* or *occasional transaction*.

17. In taking measures to verify the identity of any person purporting to act on behalf of the *customer*, the firm should take into account the *risk* posed by the *business relationship* or *occasional transaction*, the materiality of the authority delegated to the individual and the likelihood of that person giving the firm instructions concerning the use or transfer of *funds* or assets.

18. Examples of the measures the firm could take to verify the authority of a person to act could include obtaining a copy of the authorised signatories list, power of attorney or other authority or mandate providing the person with the authority to act on behalf of the *customer*.

19. The identification and verification of the identity of any person identified in accordance with Paragraph 4(3)(b) of *Schedule 3* should be undertaken in accordance with Chapters 5 and 7 of this *Handbook*.

4.3.3. The Beneficial Owner of the Customer

20. In accordance with Paragraph 4(3)(c) of *Schedule 3*, the *beneficial owner* shall be identified and reasonable measures shall be taken to verify such identity using *identification data* and such measures shall include, in the case of a *customer* which is a *legal person* or *legal arrangement*,

measures to understand the nature of the *customer*'s business and its ownership and control structure.

21. Paragraph 22 of *Schedule 3* sets out the definition of *beneficial owner*. It should be noted that the definition varies based upon the type of *legal person* or *legal arrangement* involved in a *business relationship* or *occasional transaction*. Further detail can be found in Chapter 7 of this *Handbook*.

22. For the purposes of Paragraph 4(3)(c) of *Schedule 3*, 'reasonable measures' should be read as referring to the taking of measures, which are commensurate with the *ML*, *TF* and *PF risks* which have been identified within the *business relationship* or *occasional transaction*, to understand the nature of the *customer's* business and its ownership and control structure and to verify that the *beneficial owner* of the *customer* is who he or she is claimed to be.

23. Where the *business relationship* or *occasional transaction* involves a *legal person* registered in the *Bailiwick*, the firm may have access to the beneficial ownership register maintained by the Guernsey Registry or the Alderney Registry. Whilst the beneficial ownership register is not a substitute for *CDD* measures to identify the legal person's beneficial owners, it could be useful as an additional source to validate or otherwise confirm the firm's understanding of the ownership and control structure of the customer. This position also applies to foreign beneficial ownership registers the firm may be able to access.

24. Where the *business relationship* or *occasional transaction* is a *high risk relationship*, the measures to understand the nature of the *customer's* business and its ownership and control structure will be greater than for low or standard *risk* relationships and may require the firm to ask more questions of the *customer* and require additional information about the *customer's* business and its beneficial ownership. Similarly the extent of the measures considered to be reasonable to verify the identity of the *beneficial owner* will be greater for *high risk relationships* and may require the firm to undertake more rigorous checks on the *beneficial owner* or obtain more robust forms of *identification data* to *satisfy* the firm that it has accurately verified the *beneficial owner's* identity.

4.3.4. A Person on Behalf of Whom the Customer is Acting

25. In accordance with Paragraph 4(3)(d) of *Schedule 3*, a determination shall be made as to whether the *customer* is acting on behalf of another person and, if the *customer* is so acting, reasonable measures shall be taken to identify that other person and to obtain sufficient *identification data* to verify the identity of that other person.

26. For the purposes of Paragraph 4(3)(d) of *Schedule 3*, 'reasonable measures' should be read as referring to the taking of measures, which are commensurate with the *ML*, *TF* and *PF risks* which have been identified within the *business relationship* or *occasional transaction*, to establish the identity of any natural person on whose behalf the firm has determined the *customer* is acting. Where the *risk* of the *business relationship* or *occasional transaction* is high, the extent of the measures considered to be reasonable will naturally be greater than those applied to *low risk relationships*.

27. The firm should refer to the *CDD* measures set out in Chapters 5 and 7 of this *Handbook* which the firm should take reasonable measures to apply to any person which the firm determines to fall within Paragraph 4(3)(d) of *Schedule 3*.

4.4. Policies, Procedures and Controls

28. The firm must have take-on policies, procedures and controls in place which explain how to identify, and verify the identity of, the *customer*, *beneficial owner* and other *key principals*

identified by Paragraph 4(3) of *Schedule 3* to a level appropriate to the characteristics and assessed *risk* of the *business relationship* or *occasional transaction*.

29. The firm must assess, on the basis of *risk*, how much identification information to request, what to verify, and how to verify it, in order to be *satisfied* as to the identity of a *customer*, *beneficial owner* or other *key principal*.

30. The firm's policies, procedures and controls in respect of its *CDD* measures must:

    (a) be *risk*-based to differentiate between what is expected in *low risk relationships*, what is expected in *high risk relationships* and what is expected in situations which are neither high *risk* nor low *risk*;
    (b) provide for *enhanced measures* to be applied in the circumstances where such measures are required in accordance with Paragraph 5(2) of *Schedule 3*;
    (c) impose the least necessary burden on *customers*, *beneficial owners* and other *key principals* consistent with meeting the requirements of *Schedule 3* and the *Commission Rules*;
    (d) not constrain access to financial services (for example, by those without driving licences or passports); and
    (e) deal sensibly and sensitively with special groups for whom special processes may be appropriate (for example, the elderly and students studying overseas).

31. *Identification data* providing evidence to verify identity and address can come from a range of sources, including physical or electronic *documents*, databases and electronic data sources. These sources may differ in their integrity, suitability, reliability and independence, for example, some *identification data* is issued by governments after due diligence has been undertaken on an individual's identity, i.e. national identity cards and passports, while other *identification data* may be issued with few or no checks undertaken on the subject.

32. In light of this, the firm should consider the suitability of *identification data* prior to its acceptance, including its source and whether underlying identity checks have been undertaken by the issuing body or authority. The firm should also consider the susceptibility of a *document* or source to forgery when determining its acceptability.

33. Where the firm does not receive, or have sight of, the original physical *documentation* used to verify identity (unless it uses an electronic verification system as described in Chapter 5) and where instead copy *documentation* is provided, the firm must ensure that the copy *documentation* has been electronically or physically certified by a suitable third party.

34. Further information on the policies, procedures and controls required in respect of electronic identification and verification, electronic certification and certification can be found within Chapters 5 and 6 of this *Handbook*.

35. Where the firm is not familiar with the form of the *identification data* obtained to verify identity or address, appropriate measures should be undertaken by the firm to *satisfy* itself that the *identification data* is genuine. Evidence of the steps taken by the firm should be retained as proof of its understanding and conclusions in respect of the *documents* received.

36. All key *documents* (or parts thereof) must be understood by an *employee* of the firm and that understanding must be recorded and retained with the relevant *document*.

37. The translation of *documents* should be considered on a case by case basis as it may be obvious to the firm or an *employee* in certain instances what a *document* is and what it means. The firm may also use electronic translation services including AI to translate documents, providing it is satisfied with the output. The firm may, in circumstances where the foreign language is less

familiar to it, use more than one electronic translation service to validate its understanding of the document. The firm remains responsible for the resultant product of the electronically translated documents. In all cases the firm should record its understanding of the *document* and where relevant the reason why it has not sought to translate a *document*.

38. Notwithstanding the above, the firm must translate all key *documents* (or parts thereof) into English at the reasonable request of *the Commission* or the *FIU*.

39. Where *identification data* accepted by the firm to verify the identity of a natural person contains the individual's signature and/or a photograph of the individual, the firm should ensure that the photograph and/or signature is clearly legible on the copy or scan of the *document* retained by the firm.

4.5. Timing

40. In accordance with Paragraph 7(1) of *Schedule 3*, the identification and verification of the identity of any person or *legal arrangement* pursuant to Paragraphs 4 to 6 of *Schedule 3* shall, subject to Paragraphs 4(1)(b) and 7(2) of *Schedule 3*, be carried out before or during the course of establishing a *business relationship* or before carrying out an *occasional transaction*.

41. There will be occasions when the circumstances are such that the verification of the identity of a *customer* or *beneficial owner*, cannot commence or be completed until such time as a *business relationship* has been established. This may be acceptable in certain circumstances, provided the firm is *satisfied* as to the reasons causing the delay.

42. In this respect, Paragraph 7(2) of *Schedule 3* provides that the verification of the identity of a *customer* and any of the *beneficial owners* may be completed following the establishment of a *business relationship* provided that to do so would be consistent with the *risk* assessment of the *business relationship* conducted pursuant to Paragraph 3(4)(a) of *Schedule 3*, and:

    (a) the verification is completed as soon as reasonably practicable thereafter;
    (b) the need to do so is essential not to interrupt the normal conduct of business; and
    (c) appropriate and effective policies, procedures and controls are in place which operate so as to manage *risk*, including, without limitation, a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed or the monitoring of large or complex transactions being carried outside the expected norms for that *business relationship*.

43. Paragraph 7(2) of *Schedule 3* does not, however, permit the retrospective identification of a *customer* or *beneficial owner* after the establishment of a *business relationship*, save in the circumstances detailed in Chapter 7 of this *Handbook*, for example, where beneficiaries are identified by class and are therefore unknown to the firm at the commencement of a *business relationship*.

44. Where the verification of the identity of a *customer* or *beneficial owner* takes place after the establishment of a *business relationship*, the firm must have appropriate and effective policies, procedures and controls in place so as to manage the *risk* arising from the delay. These policies, procedures and controls must include:

    (a) establishing that it is not a *high risk relationship*;
    (b) monitoring by senior management of the *business relationship* to ensure verification of identity is completed as soon as reasonably practicable; and
    (c) ensuring *funds* received are not passed to third parties.

45. The firm should be aware that there may be occasions where the circumstances are such that a *business relationship* has been established or an *occasional transaction* has been carried out and the identification and verification procedures cannot be completed. In these circumstances the firm should refer to Section 4.7. of this *Handbook*.

46. With regard to *occasional transactions*, if the identity of the *customer* is known, verification of identity is not required in the case of any transactions (whether singly or linked) below the £10,000 threshold for *occasional transactions*, or the £1,000 threshold for *occasional transactions* in the case of *virtual assets*, as set out in *Schedule 3*, unless at any time it appears that two or more transactions which appear to have been small one-off transactions are in fact linked and constitute a significant one-off transaction.

4.6. Acquisition of a Business or Block of Customers

47. There may be circumstances where the firm acquires another *specified business* with established *business relationships* or acquires from a *specified business*, or non-*Bailiwick* business, a block of *customers* that it will be servicing from *the Bailiwick*.

48. Before acquiring a business or block of *customers*, the firm must conduct enquiries on the vendor sufficient to establish the level and the appropriateness of *identification data* held in relation to the *customers* of the business to be acquired.

49. Where deficiencies in the *identification data* held are identified (either at the time of transfer or subsequently), the firm must determine and implement a programme to remedy any such deficiencies in a timely manner. The firm must also give consideration to *notifying the Commission* in accordance with the requirements of *Commission Rule* 2.63.

50. In addition to conducting due diligence on the vendor, the firm may consider it appropriate to rely on the information and *identification data* previously obtained by the vendor for its *customers* and *business relationships* where the following criteria are met:

    (a) the vendor is an *Appendix C business*;
    (b) the firm has assessed that the *CDD* policies, procedures and controls operated by the vendor were satisfactory, including consideration of the findings of any relevant reviews by *the Commission*, an overseas regulatory body (where applicable) or other third party; and
    (c) the firm has obtained from the vendor, *identification data* (or copies thereof) for each *business relationship* acquired.

51. Where the firm disposes of a book of business, it should ensure that the record keeping requirements of Paragraph 14 of *Schedule 3* and the *Commission Rules* in Chapter 16 of this *Handbook* are met in respect of the business being disposed of.

4.7. Failure to Complete Customer Due Diligence

52. In accordance with Paragraph 9 of *Schedule 3*, where the firm can not comply with any of Paragraph 4(3)(a) to (e) or Paragraph 11(1)(a) to (b) of *Schedule 3* it shall:

    (a) in the case of an existing *business relationship*, terminate that *business relationship*;
    (b) in the case of a proposed *business relationship* or *occasional transaction*, not enter into that *business relationship* or carry out that *occasional transaction* with the *customer*; and
    (c) consider whether a disclosure must be made pursuant to Part I of *the Disclosure Law*, or Sections 15 or 15A, or Section 12 (as appropriate) of *the Terrorism Law*.

53. It is recognised that the immediate *termination* of a *business relationship* may not be possible due to contractual or legal reasons outside the control of the firm. The timing of the *termination* of an established *business relationship* will also depend upon the nature of the underlying products or services. As an example, while a *bank* can close an *account* and return deposited *funds* to a *customer* relatively easily, the compulsory redemption of an investment in a CIS, particularly where it is closed-ended or where valuation dates are infrequent, may be more problematic.

54. Where *termination* of a *business relationship* cannot be completed (for example, because the firm has lost contact with the *customer*) the firm should have procedures and controls in place to ensure that assets or *funds* held are 'blocked' or placed on a 'suspense' *account* until such time as contact with the *customer* is re-established or the firm has otherwise dealt with the *funds* or assets in accordance with its policy for dormant *accounts*.

55. Where the immediate *termination* of a *business relationship* is not possible for whatever reason, the firm must ensure that the *risk* is managed and mitigated effectively until such time as the *business relationship* can be terminated.

56. The firm must ensure that where *funds* have already been received, they are returned to the source from which they originated, regardless of whether the source is the *customer* or a third party. Where the firm has been unable to return the *funds* to the *account* from which they were received, for instance because the originating *bank account* has been closed, the firm must take appropriate steps to return the *funds* to the same party in another form.

57. Where this is not possible (for example, if the relevant party no longer exists) the firm should take appropriate steps to return any *funds* to an appropriate third party and document the reasoning for the steps taken.

58. Where the firm has terminated, or not proceeded with establishing, a *business relationship* or *occasional transaction*, it must consider the circumstances giving rise to the failure to complete *CDD* measures and whether these warrant a disclosure to the *FIU*.

4.8. Collective Investment Schemes

4.8.1. Responsibility for Investor CDD

59. As part of the process of applying to *the Commission* for the authorisation or registration of a closed-ended CIS ("CECIS") or open-ended CIS ("OECIS"), the board of the CIS (or General Partner ("GP") of a Limited Partnership ("LP"); trustee of a unit trust; or *foundation official* of a *foundation* as appropriate) will nominate a firm (the "*nominated firm*") which is licensed under *the POI Law* and contracted to, or connected with, the CIS either as its manager or designated administrator, to be responsible for meeting the requirements of *Schedule 3* and this *Handbook* for investors into the CIS, in addition to its own obligations. Where the authorisation/registration of a CIS is suspended, it remains authorised/registered for the purposes of the *POI Law* and, as such, will continue to maintain a *nominated firm*. In cases where a third party liquidator is appointed to a CIS whose authorisation/registration has been suspended, and that liquidator is registered with *the Commission* as a *prescribed business*, *the Commission* will consider a request from the liquidator to be appointed as the *nominated firm* of the CIS.

60. The *nominated firm* must advise *the Commission* that it has been so nominated during the course of the application process, and in any case prior to the authorisation or registration of the CIS.

61. The *nominated firm* must treat all investors into the CIS as if they were its *customers* and ensure that the relevant provisions of *Schedule 3* and this *Handbook* are met, for example, conducting

relationship risk assessments and identifying, and verifying the identity of, the investors, including the *beneficial owners* and other *key principals* thereof.

62. Whilst the application of *CDD* measures (including *ECDD* and *enhanced measures* as necessary) may be undertaken by another party (for example, under an outsourcing arrangement) the *nominated firm* will be responsible for ensuring that appropriate *identification data* is held on all investors, including the *beneficial owners* thereof, which meets the relevant requirements of *Schedule 3* and this *Handbook*.

63. Where the *nominated firm* provides services to a CIS, the shares of which are traded on a stock exchange, the *nominated firm* should refer to the provisions of Section 4.8.3. of this *Handbook.*

64. Where the firm provides services to a CIS and has not been nominated under Paragraph 4.59. above, the firm should treat the CIS as its *customer* and conduct *CDD* in accordance with the requirements for a CIS authorised or registered by *the Commission*.

65. There may be occasions where the *nominated firm* will change throughout the life of a CIS, for example, as a result of a change of designated administrator. Where the firm becomes the nominated firm for a CIS which has already been authorised or registered by *the Commission*, it must advise *the Commission* in writing that it has been so nominated as soon as reasonably practicable after its nomination.

66. Where the firm becomes nominated for a CIS with existing investors, the firm should give consideration to the requirements of Section 4.6. of this *Handbook.*

67. Notifications made in accordance with *Commission Rule* 4.65. should be submitted via the Commission's Online Submissions Portal, through the completion of a Form 235. Liquidators requesting appointment as a *nominated firm* should do so through completion of a Form 200.

https://submit.gfsc.gg/

4.8.2. Identifying and Verifying the Identity of Investors in Collective Investment Schemes

68. This Section details the obligations for the application of *CDD* measures to investors, including the *beneficial owners* thereof, and applies where the firm:

(a) has been nominated under Paragraph 4.59. of this *Handbook;* or
(b) is acting in the capacity of the administrator or *transfer agent* of a non-Guernsey CIS ("NGCIS"), unless the contractual arrangements for the services provided by the firm require otherwise.

69. Fundamental to understanding the *CDD* obligations for CIS investors is a recognition that the overall arrangements by which interests in a CIS are offered to investors, together with the arrangements under which a CIS consequently deals with investors, will determine the *CDD* measures to be applied.

70. When undertaking its responsibilities, the firm should be mindful of the vulnerabilities of CISs and the methods by which CISs may be used by persons or entities for *ML, TF* and/or *PF* purposes. For example:

(a) CISs are often distributed on a non-face-to-face basis, with access to those CISs (particularly where they are OECISs) relatively quick and easy to achieve, together with an ability for holdings to be transferred between different parties;

(b) OECISs, particularly those with frequent (i.e. daily or weekly) dealing, can provide the ability for short holding periods and the high turnover of share/unit purchases/redemptions; and

(c) Notwithstanding the often medium to long-term nature of CISs, which can contribute to limiting the attractiveness of these products for *ML* purposes, they may still appeal to money launderers on the basis of their ability to generate growth and income.

71. Investments into a CIS will generally fall into one of four broad categories, each presenting its own *risks* and having its own obligations in respect of the *CDD* measures to be applied. *Commission Rule* 4.72. below sets out the party to be treated as the *customer* and the *CDD* measures to be applied to that *customer* (including the *beneficial owner* thereof) for each category of investment.

72.	Method of Investment	Party to be Treated as the Customer
(a)	A natural or *legal person* or *legal arrangement* directly purchasing units of, or shares in, a CIS on their own *account*, and not on behalf of other, underlying parties.	The firm must treat the investor as if it were its *customer* and apply *CDD* measures (including *ECDD* and/or *enhanced measures* as applicable) to the investor, including the *beneficial owner* of that investor, in accordance with the requirements of *Schedule 3* and this *Handbook*.
(b)	An investor that, as part of its economic activity, directly purchases the units of, or shares in, a CIS in its own name and exercises control over the investment for the ultimate benefit of one or more third parties who do not control the investment or investment decisions and where *funds* (and any related income) arising from the investment in the CIS will only be returned to the registered owner of the shares or units in the CIS.	In both scenarios (b) and (c), where the investor is an *Appendix C business* acting as an *intermediary* for one or more third parties, the firm can treat the investor (i.e. the *intermediary*) as the *customer*, provided the relationship has been assessed as low *risk* and the requirements of Section 9.8. of this *Handbook* are met. Where the *intermediary relationship* has been assessed as being other than low *risk*, the firm cannot treat the *intermediary* as its *customer* and *CDD* measures (including *ECDD* and/or *enhanced measures* as applicable) must also be applied to the underlying investors (i.e. the *intermediary's* customers), including the *beneficial owners* thereof, in accordance with the requirements of *Schedule 3* and this *Handbook*.
(c)	An investor, for example a financial intermediary, that acts in its own name and is the registered owner of the shares or units but acts on the *account* of, and pursuant to specific instructions from, one or more third parties and where *funds* (and any related income) arising from the investment in the CIS will only be returned to the registered owner of the shares or units in the CIS.	
(d)	A business' *customer*, for example a financial intermediary's *customer*, where the business is not the registered owner of the shares or units (for example, because the CIS uses a financial intermediary to distribute fund shares or units, and the investor purchases units or shares through the business and the business does not become the legal owner of the units or shares).	The firm must treat the underlying investor, i.e. the intermediary's customer, as if it were its *customer* and apply *CDD* measures (including *ECDD* and/or *enhanced measures* as applicable) to the investor, including the *beneficial owner* thereof, in accordance with the requirements of *Schedule 3* and this *Handbook*. Where the intermediary meets the definition of an *Appendix C business*, the firm could consider treating the intermediary as an *introducer*, provided the requirements of Chapter 10 of this *Handbook* are met.

4.8.3. Collective Investment Scheme Traded on a Recognised Stock Exchange

73. This Section relates to authorised and registered CISs, constituted as companies, whose shares are listed and traded on recognised stock exchanges like those of other publicly held companies, such as investment trusts and exchange traded funds ("traded CISs").

74. This approach is recognised by IOSCO in its Anti-Money Laundering Guidance for Collective Investment Schemes issued in October 2005, which states:

> "Closed-ended exchange-listed CISs are just like any other public company that lists its shares on an exchange, and public companies – other than financial institutions – do not have specific anti-money laundering responsibilities".

75. With regard to such publicly listed companies, the FATF sets out its position on the treatment of listed companies in its Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems dated February 2013, which states that:

> "Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies. The relevant identification data may be obtained from a public register, from the customer or from other reliable sources".

76. The shares of a traded CIS are not sold or traded directly with investors, but are issued, distributed and traded through placing agents, broker/dealers and other market intermediaries to individual and corporate investors. As such, a traded CIS and the *nominated firm* thereof do not have the same opportunity to engage with investors prior to accepting an investment, approving a transfer or undertaking a corporate action such as a share buy-back or dividend distribution.

77. Where the shares of a CIS are traded on a recognised stock exchange within the meaning of *the Beneficial Ownership Regulations*, in accordance with Paragraph 4(4) of *Schedule 3* it is not necessary for the firm nominated by that CIS under Paragraph 4.59. to identify, and verify the identity of any of the investors in that scheme.

78. Where the firm has been nominated under Paragraph 4.59. for a traded CIS, it must understand the routes by which investors could enter the CIS and have considered the *risk* presented by these routes to entry in its risk assessment of the CIS carried out under Paragraph 3(4) of *Schedule 3* and this *Handbook*.

Chapter 5
Natural Persons

Contents of this Chapter

5.1. Introduction

1. The purpose of this Chapter is to set out the information to be obtained, as a minimum, for a natural person who acts as a *key principal* in one or more of the following capacities within a *business relationship* or *occasional transaction*:

   (a) the *customer*;
   (b) the *beneficial owner* of the *customer*;
   (c) a natural person purporting to act on behalf of the *customer*; or
   (d) a natural person on behalf of whom the *customer* is acting.

2. Establishing that a natural person falling within Paragraph 4(3) of *Schedule 3* as set out above is the person that he or she claims to be is a combination of being satisfied that:

   (a) the person exists, based on the accumulation of information about the person's identity; and
   (b) the *customer*, *beneficial owner* or other *key principal* is that person, by verifying from *identification data*, satisfactory confirmatory evidence of that person's identity.

3. This Chapter sets out the aspects of a natural person's identity which must be established, together with the characteristics of that natural person's identity to be verified using *identification data*, in order to comply with the requirements of *Schedule 3*.

4. The requirements of this Chapter apply:

   (a) when establishing a *business relationship;*
   (b) when carrying out an *occasional transaction*; and
   (c) where any of the parties set out above to a *business relationship* change throughout the life of that relationship.

5.2. Identifying Natural Persons

5. Where the firm is required to identify a natural person falling within Paragraph 5.1. above, it must collect relevant information on the identity of that natural person which includes:

   (a) legal name;
   (b) any former names (such as maiden name) and any other names used;
   (c) principal residential address;
   (d) date and place of birth;
   (e) nationality (including all nationalities where the individual holds more than one); and
   (f) any occupation, public position held and, where appropriate, the name of any employer.

6. In accordance with Paragraph 4(3)(f) of *Schedule 3*, as part its *CDD* measures the firm shall make a determination as to whether the *customer* or *beneficial owner* is a *PEP* and, if so, whether he or she is a *foreign PEP*, a *domestic PEP* or *international organisation PEP*.

7. Further information on the identification and treatment of *PEPs* can be found in Section 8.5. of this *Handbook*.

5.3. Verifying the Identity of Natural Persons

8. Subject to Section 9.3. of this *Handbook*, the firm must verify a natural person's identity using *identification data*, the extent of which is to be determined based on the conclusion of the *relationship risk assessment*. As a minimum, the firm must verify:

   For all natural persons:

   (a) legal name;
   (b) date of birth; and
   (c) residential address.

   For natural persons connected with *business relationships* or *occasional transactions* which are other than low *risk*, additionally:

   (d) place of birth; and
   (e) nationality.

9. In order to verify the above and other information collected, the following *identification data* is considered to be the best possible:

   (a) current passport, bearing a photograph of the natural person;
   (b) current national identity card, bearing a photograph of the natural person;
   (c) armed forces identity card, bearing a photograph of the natural person;
   (d) driving licence, bearing a photograph of the natural person; or
   (e) independent data sources (including electronic sources) (see Section 5.7. below).

10. The examples quoted above are not exclusive. There may be other forms of *identification data* of an equivalent nature which may be produced as satisfactory evidence of the identity of a natural person.

11. Regardless of its form, the firm must be *satisfied* as to the validity and veracity of the *identification data* used to verify the identity of a natural person and its evidential value should be based on the assessed *risk* of the *business relationship* or *occasional transaction*. In this respect, the firm should be aware that certain *documents* may be more susceptible to fraud than others, or have less robust controls in respect of their issue, for example, some jurisdictions may issue driving licences without due diligence being undertaken on the holder.

12. When changes occur which result in a modification to a natural person's profile (for example, a change of name) the firm should apply a *risk*-based approach to updating that person's *CDD* records and consider what, if any, additional *identification data* is required to verify the change.

13. In addition to the measures set out above, where the firm has determined that a *business relationship* or *occasional transaction* is high *risk*, in accordance with Paragraph 5(1) of *Schedule 3* the firm shall also apply *ECDD* measures to that *business relationship* or *occasional transaction*. Those *ECDD* measures shall include, inter alia, taking one or more steps as would be appropriate to the particular *business relationship* or *occasional transaction* and could include, in accordance with Paragraph 5(3)(a)(v)(B) of *Schedule 3*, verifying additional aspects of the *customer's* identity.

14. Examples of additional aspects of the *customer's* identity that the firm could verify, where that *customer* is a natural person, include his or her occupation or any former name(s). Further detail in respect of *ECDD* measures can be found in Chapter 8 of this *Handbook*.

5.4. Verification of Residential Address

15. The following are examples of suitable methods to verify the residential address of a natural person:

(a) a recent *bank*/credit card statement or utility bill;
(b) correspondence from an independent source such as a central or local government department or agency (in *the Bailiwick* and the Bailiwick of Jersey this will include States departments and parish authorities);
(c) commercial or electronic data sources;
(d) a letter from an *Appendix C business* with which the individual has an existing *business relationship* and which confirms residential address;
(e) a tenancy agreement;
(f) a personal visit to the residential address; or
(g) an electoral roll.

16. Where a natural person's principal residential address changes during the course of a *business relationship*, the firm is considered to have verified the new address where it has maintained on-going written correspondence with the natural person at that new address (i.e. it has sent and subsequently received responses to written correspondence addressed and sent by post to the new address).

5.4.1. Overseas Natural Persons

17. There may be occasions when a natural person who is not resident in *the Bailiwick* is unable to provide evidence of his or her residential address using the means set out in Paragraph 5.15. above. Examples of such individuals include residents of countries without postal deliveries or street addresses who rely on post office boxes or an employers' addresses for the delivery of mail.

18. Notwithstanding the above, it is essential for law enforcement purposes that a record of a natural person's residential address (or details of how that person's place of residence can be reached) is held by the firm. As such, it is not acceptable to simply record details of a post office box number as a natural person's address.

19. Where the firm has determined that an individual has a valid reason for being unable to produce more usual *documentation* to verify their residential address and who would otherwise be excluded from establishing a *business relationship* or undertaking an *occasional transaction* with the firm, the residential address can be verified by other means, provided the firm is *satisfied* that the method employed adequately verifies the address of the natural person and any additional *risk* has been appropriately mitigated.

20. An example of such an alternative method could be a letter from a director or officer of a reputable overseas employer confirming residence at a stated overseas address (or providing detailed directions to locate a place of residence).

5.5. Online Bank Statements or Utility Bills

21. Where the residential address of a natural person is to be verified through the use of a *bank*/credit card statement or utility bill, the default option is to obtain a form of verification which has been delivered to that natural person by post. However, the receipt of such items via the traditional postal system has largely been replaced by online billing, the delivery of *bank* or utility statements via e-mail (an "electronic statement") or through logging on to the bank/card issuer's customer portal.

22. Examples of electronic statements include:

(a) an online statement issued by a recognised *bank*, building society, credit card company or recognised lender bearing the name and residential address of the natural person; or
(b) an online bill in relation to rates, council tax or utilities bearing the name and residential address of the natural person.

23. Where the firm wishes to accept an electronic statement as verification of a natural person's address, it must be *satisfied* as to the validity and veracity of the electronic statement presented.

24. The firm should recognise that some electronic sources may be more easily tampered with, i.e. the data contained within them subject to amendment, than others. If suspicions are raised in relation to the integrity of any electronic statement obtained, the firm should take whatever practical and proportionate steps are available to establish whether these suspicions are substantiated, and if so, whether the relevant electronic statement should be accepted.

25. An example of a step the firm could take where it has concerns over the veracity of a *document* is to corroborate the content of that *document* using an independent source, for example, a commercial or electronic data source such as a land registry, electoral roll or similar.

5.6. Electronic Verification

26. Electronic verification is the use of an electronic method or system to verify, in whole or in part, the identity of a natural person by matching specified personal information against electronically captured physical *documentation* and/or independent electronic data sources through verification technology.

27. An assessment of the risks associated with using such technology should be undertaken in accordance with Paragraph 3(3)(c)(ii) of Schedule 3 and the rules and guidance in both section 3.12 of Chapter 3 and the rules in this section of this *Handbook* in advance of adopting an electronic verification system to verify a customer's identity.

28. A firm must, when undertaking a technology risk assessment of an electronic verification system in accordance with Paragraph 3(3)(c)(ii) of Schedule 3, document the identity data and information that it collects about the customer, the nature of the data sources to be used (such as a current passport) and how their authenticity is assessed by the system.

29. Electronic verification can be used to verify all or any combination of the mandatory data points required by *Commission Rule* 5.8. Where an electronic verification system does not fulfil all of these requirements, the firm must use one or more other methods to ensure that a natural person is fully verified in accordance with the requirements of this *Handbook*.

30. Electronic verification systems range in scope from the electronic capture of identity information and *identification data* on a face-to-face basis through to the self-capture of uncertified *documentation* by a natural person using an interactive application ("App") on a tablet or mobile phone. In the latter example, a photograph (or a series of photographs or a video) of the natural person are obtained through the App, together with photographs of *identification data* and address verification *documents*. The photographs are then independently reviewed and corroborated constituting the verification.

31. Whilst the use of electronic verification can help to reduce the time and cost involved in gathering information and *identification data* for a natural person, the firm should be mindful of any additional *risks* posed by placing reliance on an electronic method or system. This should include understanding the method and level of review and corroboration within the system and the

potential for the system to be abused, particularly through the advancement of AI derived "deepfakes" or synthetic identities. The FATF issued an "horizon scan" in December 2025 warning how criminals can exploit new technologies, including AI, to facilitate their illicit activities.

https://www.fatf-gafi.org/en/publications/Methodsandtrends/horizon-scan-ai-deepfake.html

32. Knowledge and understanding of the functionality and capabilities of a system can help provide assurance of its suitability. In particular, there should be certainty of the methods applied to corroborate *identification data*. The use of more than one confirmatory source to match data enhances the assurance of authenticity.

33. The firm's technology risk assessment must consider and document the measures within the electronic verification system which address the risk of identification data being forged or tampered with, including through manufactured audio-visual media content to create synthetic identities (i.e. "deepfakes") The assessment must be reviewed at least annually to ensure it remains current with technological developments.

34. In addition to the rules and guidance for technology risk assessments set out in section 3.12 of this *Handbook*, a firm should consider the following factors when undertaking an assessment of an electronic verification system:

a) the clarity and resolution of the electronic copy to detect its security features such as a watermark, invisible ink, hologram or the fraudulent insertion of a photograph or data;
b) how the system tests the authenticity of the electronic document, such as through biometric data comparison, live stream facial recognition, reading data on the document's electronic chip, analysis of security features and geotagging/geolocation confirmations;
c) whether the process for copying and transmitting the electronic document to the firm presents an opportunity for the document to be tampered with or manipulated;
d) the level of security over the process of transmitting the document, including application of security codes or anti-impersonation measures, such as requirements for the natural person to verbally repeat words, perform an action or use passcodes etc.;
e) the service provider's policy for testing the veracity and security of the system from cyber-attacks and in response to the criminal development of technology to create synthetic identities/deepfakes;
f) clearly documenting how identity information and addresses are verified, for example, biometric matching of an individual in a live video to an identity document which also has anti-fraud and authenticity checks conducted on it, or searching through multiple independent sources within a specified date range for address verification etc.; and
g) the extent to which a user, or the firm, is able to bypass any built-in security features of the electronic process, or adapt the system's use beyond that intended by the service provider.

35. Whether the firm uses an in-house, group or third-party system, it should periodically question and seek assurance that the system continues to remain robust in the face of developments in the criminal exploitation of technology, including being informed of any advanced identification measures which have been introduced.

36. The firm must ensure that sufficient customer records to comply with the record-keeping requirements under Paragraph 14 of Schedule 3 and rules on Chapter 16 are available to, and readily retrievable by, the firm for the *minimum retention period*.

37. Customer records verified through electronic verification systems should detail the identity checks undertaken by the system, and the sources it used. This is usually provided in a system generated report.

38. The firm must ensure that its CDD policies, procedures and controls and its compliance monitoring programme include its use of electronic verification, where used.

39. Video calls have a role in customer due diligence in enabling the firm to discuss aspects of a new business application or proposed transaction with an existing customer. Firms should be mindful that criminals are employing increasingly sophisticated techniques to forge identity documents therefore relying solely on video calls without independent verification could expose firms to these increased risks. Selfie-photographs of the natural persons with their identity document are also not an acceptable means for verifying their identity.

40. Further information on the certification of *identification data* received via an electronic verification system can be found in Section 6.5. of this *Handbook*.

5.7. Independent Data Sources

41. *Identification data* does not have to be in paper form. Independent data sources can provide a wide range of confirmatory material on natural persons and are becoming increasingly accessible, for example, through improved availability of public information and the emergence of commercially available data sources such as electronic databases and research firms. Sources include:

(a) electoral roll;
(b) telephone directories;
(c) credit reference agency checks;
(d) business information services; and
(e) electronic checks provided by commercial agencies.

42. Where the firm is seeking to verify the identity of a natural person using an independent data source, whether by accessing the source directly or by using an independent third party organisation (such as a credit reference agency), an understanding of the depth, breadth and quality of the data is important in order to determine that the method of verification does in fact provide satisfactory evidence of identity.

43. Independent data sources can be used to verify all or any combination of the mandatory data points required by *Commission Rule* 5.8. Where an independent data source does not fulfil all of these requirements, the firm must use one or more other methods to ensure that a natural person is fully verified in accordance with the requirements of this *Handbook*.

44. When relying on independent data sources to verify identity, the firm should ensure that the source, scope and quality of that data is suitable and sufficient and that the process provides for the information to be captured and recorded.

5.8. Guarding Against the Financial Exclusion of Bailiwick Residents

45. There may be occasions when a *Bailiwick* resident natural person encounters difficulties in providing evidence of his or her *Bailiwick* residential address using the sources identified previously in this Chapter. Examples of such circumstances include:

(a) a Short-Term Employment Permit holder who does not have a permanent residential address in *the Bailiwick*;
(b) a natural person living in *the Bailiwick* in accommodation provided by that person's employer, with family (for example, in the case of minors), or in care homes, who may not pay directly for utility services; or

(c) a *Bailiwick* student living in university, college, school, or shared accommodation, who may not pay directly for utility services.

46. Where a natural person has a valid reason for being unable to produce the requested *documents* and who would otherwise be excluded from accessing the firm's products and services, identification procedures should provide for alternate means of verifying a natural person's *Bailiwick* residential address. The following are examples of alternate methods of verifying an address:

(a) a letter from the head of the household at which the natural person resides confirming that the applicant lives at that *Bailiwick* address, setting out the relationship between the natural person and the head of the household, together with evidence that the head of the household resides at the address;
(b) a letter from the residential home or care home confirming residence of the natural person;
(c) a Resident Certificate or Resident Permit;
(d) a letter from a director or manager of *the Bailiwick* employer confirming residence at a stated *Bailiwick* address and indicating the expected duration of employment. In the case of a Short-Term Employment Permit holder, the worker's residential address in his or her country of origin should also be obtained and reasonable measures taken to verify that address; or
(e) in the case of a *Bailiwick* student, a letter from a *Bailiwick* resident parent or a copy of the acceptance letter for a place at the college/university. The student's residential address in *the Bailiwick* should also be obtained and reasonable measures taken to verify that address.

Chapter 6
Electronic & Physical Certification and Electronic ID&V

Contents of this Chapter

6.1. Introduction

1. Certification is the process whereby, instead of a natural person presenting his/her self and *identification data* in person to the firm, the individual uses a suitable trusted third party to confirm a positive link between his/her identity and *identification data*. The certified *identification data* is then provided to the firm as verification of that natural person's identity.

2. The use of third party certification serves to mitigate the *risk* arising from a *business relationship* or *occasional transaction* where the firm has had no face-to-face contact with a natural person who is a *key principal* within that relationship. It also guards against the risk that *identification data* provided is fraudulent or misleading and does not correspond to the individual whose identity is to be verified.

3. Certification has two purposes:

   (a) to provide assurance to the firm that a natural person is who he or she purports to be; and
   (b) to confirm that the natural person is the owner of the *identification data* used for the purpose of the firm verifying identity.

4. Until recently, certification has required that trusted third parties are natural persons of sufficient professional standing and subject to appropriate ongoing requirements in respect of their integrity. However, with developments in technology the trusted third party could now take the form of an electronic system which, through the integration of controls such as those detailed later in this Chapter, can provide sufficient corroboration equivalent to that provided by a natural person certifier.

5. This Chapter is split into three sections and provides distinct requirements for certification depending upon the method of certification to be used:

   (a) natural persons certifying hard-copy *identification data*;
   (b) natural persons certifying scanned *identification data* by the application of an electronic signature; and
   (c) electronic methods of certifying *identification data*.

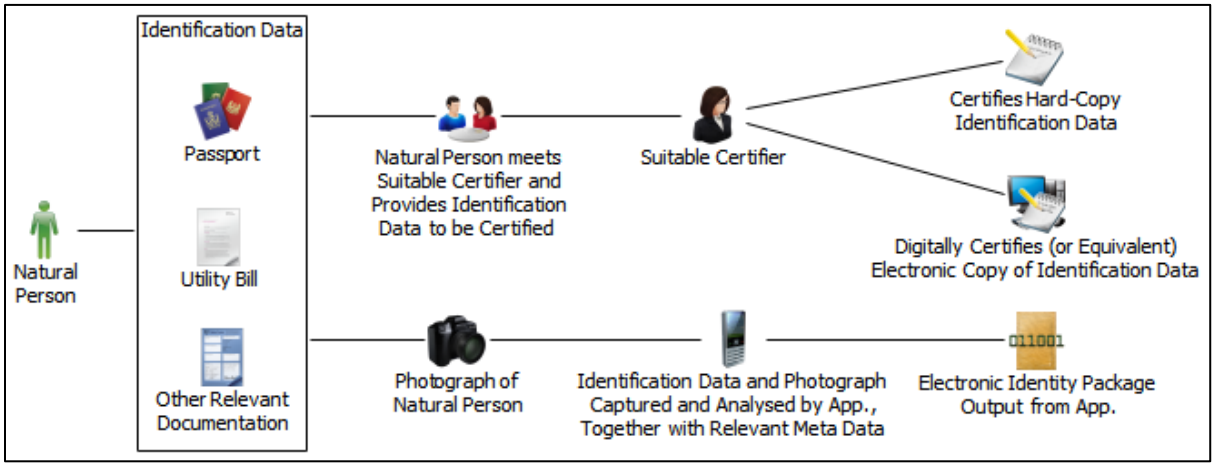


Fig. 2, Process of Certification

6.2. Obligations

6. For certification to be effective, the certifier should be a trusted third party who, in the case of natural person certification, has seen the original *identification data* and, where that *identification*

data includes a photograph, met the individual in person. Only following these two steps can the certifier provide the necessary assurance to the firm about the individual's identity.

7. In order to ensure this effectiveness, the firm should have as part of its compliance arrangements:

   (a) a policy and/or procedures which reflect the firm's *risk* appetite towards relying upon certified *identification data*;
   (b) a policy in relation to those third parties considered by the firm to constitute suitable certifiers; and
   (c) procedures allowing for the firm to verify the suitability of those third parties who have certified *identification data* upon which the firm intends to rely.

8. The firm must exercise caution when accepting certified *identification data*, especially where such *identification data* originates from a country or territory perceived to represent a high *risk*, or from unregulated entities in any country or territory.

6.3. Requirements for Natural Person Certifiers

9. Whilst there is no specific wording to be used by the certifier, the firm must ensure that the certifier signs and dates the certification and provides sufficient information within the certification or accompanying the certification for the firm to confirm the following:

   (a) that the certifier has seen the original *identification data* verifying identity or residential address;
   (b) that the certifier has met the natural person who is the subject of the *identification data;* and
   (c) adequate information about the certifier in order that the firm can undertake the required assessment of the suitability of the certifier and so that contact can be made with the certifier in the event of a query.

10. The certification should be provided by the certifier either on a copy of the *identification data* which is the subject of the certification or attached to that *document* by way of a covering letter or other record which accompanies the *identification data*. Where information in *Commission Rule* 6.9 above has not been provided on, or attached to, the *identification data*, it can be supplemented, for example by additional correspondence with the certifier, without the need to obtain renewed copies of the *identification data*. In this case, the additional correspondence forms part of the *CDD information* and the respective record-keeping requirements should be applied.

11. For the purposes of *Commission Rule* 6.9.(c) 'adequate information' should include:

   (a) the full name of the certifier;
   (b) the professional position or capacity held by the certifier (including professional body membership details where relevant); and
   (c) details of at least one contact method (for example, postal address, contact telephone number and/or e-mail address).

12. Certification by a natural person can take two forms;

   (a) paper-based certification where the certification is stamped or written onto a photocopy of the *identification data* or attached thereto; or
   (b) where hard-copy *identification data* is scanned and certified by application of a signature in electronic form (as defined in the Electronic Transactions (Guernsey) Law, 2000) from the natural person to an electronic copy of the *identification data*.

For the avoidance of doubt, obtaining identification data that has been certified in accordance with 6.12(b) above will be as acceptable as, and equivalent to, obtaining paper-based certification as detailed in 6.12(a) above.

13. The process for utilising an electronically signed copy of *identification data* which certifies its authenticity mirrors that for paper-based documentation as set out in Paragraph 6.12.(a) above. If the certifier accepts the *identification data* presented by the *customer*, then using electronic encryption or a suitably robust alternative, the certifier will apply a signature in electronic form (or equivalent) to an electronic copy of the *identification data*. This encrypted file is then provided electronically to the firm. This is as acceptable as a "wet-ink" or physical signature.

14. Where the firm accepts an electronic copy of the *identification data* which has been certified by a natural person applying his or her signature electronically, it must *satisfy* itself as to the veracity of the certification process leading to the natural person's decision to certify the *identification data*.

15. The above rule is designed to ensure the firm understands the basis upon which a certifier has met the person whose identity they are certifying and it is not a requirement to understand the underlying technology used within systems to certify the documents.

16. Where the firm wishes to accept soft-copy certified *identification data*, the preference should be to receive electronically certified (or equivalent) *identification data* using the process set out in Paragraphs 6.12.(b) to 6.14. above. However, there may be situations where the certifier does not have access to such technology, or is otherwise unable to electronically certify *documents*, and where the provision of hard-copy documentation via the postal system is unfeasible or uneconomical.

17. Where the firm receives *identification data* covered by Paragraph 6.12.(a) in scanned soft-copy form, the firm must be *satisfied* as to the veracity of the *identification data* provided and that the receipt of such *identification data* in soft-copy form does not pose an increased *risk* to the firm.

18. In *satisfying* itself as to the veracity of the scanned soft-copy *identification data* received, the firm should consider, amongst other factors, the type of *identification data* used (for example, is it known to be easily manipulated) and the source of the document(s) received (for example, were they provided by the subject of the *identification data*, or by an independent source such as the certifier or a representative thereof).

6.4. Assessing the Suitability of Natural Person Certifiers

19. Where copy *identification data* certified by electronic or physical signature is accepted, regardless of the manner or form of the *identification data*, the firm must *satisfy* itself that the certifier is a suitable and appropriate person to provide validation of the *identification data* based on the assessed *risk* of the *business relationship* or *occasional transaction*, together with the level of reliance being placed on the certified *documents*.

20. The firm should, as part of its compliance arrangements, have in place a policy which enables it to determine whether an individual is suitable to certify *documents* and therefore whether reliance can be placed upon the certified *identification data* provided. The policy should take account of factors including whether the certifier:

    (a) is closely related or otherwise connected to the person whose identity is being certified;
    (b) holds an appropriate public position with a high level of trust and for which background checks or similar vetting of the certifier's fitness and propriety will have been undertaken;

(c) is a member of a professional body which undertakes independent oversight of compliance with its own rules or standards of professional conduct;
(d) is required to satisfy criteria similar to the 'fit and proper' requirements of the minimum licensing criteria in *the Bailiwick* and is required to be vetted or approved as part of the regulation in the jurisdiction in which it operates;
(e) is employed by another business forming part of a group of which the firm is also a member where the same or equivalent AML and CFT policies, procedures and controls apply; or
(f) is subject to other professional rules or a member of an industry body (or equivalent) providing for the integrity of the certifier's conduct.

21. The firm's policy for assessing the suitability of a certifier should include consideration of the circumstances where the firm deems it appropriate to validate the credentials of the certifier.

22. As part of the steps taken to validate the credentials of a certifier, the firm may also include the consideration of factors such as:

(a) the reputation and track record of the certifier;
(b) the firm's previous experience of accepting certified *documents* from persons in the same profession or country or territory;
(c) the adequacy of the framework to counter *ML* and *FT* applicable in the country or territory in which the certifier is located; and
(d) the extent to which the framework applies to the certifier.

6.5. Certification Requirements for Copies of Identification Documents Verified Through Electronic System Certifiers

23. In addition to accepting copies of identification data certified by electronic or physical signature in accordance with the aforementioned rules in this Chapter, the firm may also accept copies of identification data which have been certified as a true copy by a regulated firm which has verified the person through an electronic verification system. Sections 5.6. and 5.7. of this *Handbook* provide more detail about an electronic verification system's role in verifying a natural person's identity.

24. A firm may accept copies of identification data certified as a true copy of the original *identification data* from a firm which is subject to AML/CFT supervision by a competent authority, provided that the firm providing the copy *identification data* certifies that the natural person is its customer or a *key principal* of its customer and that the certifying firm has downloaded the document from an electronic verification system which it uses.

25. The firm must establish that the certifying firm is supervised for compliance with AML/CFT measures. There is no specific wording for the certification, but it must be sufficient to ascertain that:

a) the natural person is a customer or *key principal* to a customer of the certifying firm;
b) the document is a true copy of the identification data verified by the electronic verification system the certifying firm uses; and
c) the copy of the *identification data* has been downloaded from an electronic verification system used by the certifying firm.

6.6. Certification of Documentation for Legal Persons and Legal Arrangements

26. Where the firm is provided with *documents* to verify the identity of a *legal person* which are copies of the originals, the firm must ensure they have been certified by the company secretary, director, manager or equivalent officer, or by a suitable third party certifier.

27. Where the firm is provided with *documents* to verify the identity and legal status of a *foundation* which are copies of the originals, the firm must ensure they are certified by a *foundation official* or by a suitable third party certifier.

28. Where the firm is provided with *documents* to verify the identity and legal status of a trust or other *legal arrangement* which are copies of the originals, the firm must ensure they are certified by a representative of the trustee (or equivalent) or by a suitable third party certifier.

29. Certification should be provided in a similar form to that set out under Section 6.3. of this Chapter, either through the certifying of a hard-copy *document*, or through the use of a signature in electronic form (or equivalent) applied to an electronic copy of the *document*.

30. While there are no specific requirements in respect of the wording used, the firm must *satisfy* itself that the natural person certifying the *document* is a suitable and appropriate person within the specific circumstances of the *business relationship* or *occasional transaction*.

6.7. Chains of Physical Copy Certified Documentation

31. As detailed previously, the acceptance of original *identification data*, or *identification data* which has been certified in accordance with this Chapter, serves to protect the firm from the *risk* of it relying upon *identification data* which is fraudulent or misleading, or which does not correspond to the individual whose identity is to be verified. The benefits of this mitigation are limited, however, where *documents* have passed through a chain of certifiers (for example, other *FSBs*) and the link between the *customer* (or other *key principal*) and the firm has become distant.

32. Noting this concern, the firm should not place reliance upon copies of certified copies of original *identification data*, other than in justifiable instances. The firm should always consider the risk of placing reliance upon copies of certified copies of *identification data* and consider whether it would be more appropriate to obtain the original, or original certified copies of, *identification data*.

33. For the purposes of Paragraph 6.32. above, examples of justifiable instances include:

    (a) the provision of copies of *identification data* held by the trustee of a trust in respect of the *beneficial owners* of that trust to a *bank* for the purposes of opening an *account* on behalf of that trust; or
    (b) the provision of copies of *identification data* held by an *Appendix C business* to a legal professional engaged by the *Appendix C business* to provide advice in connection with a *customer* of, and at the request of, the *Appendix C business*.

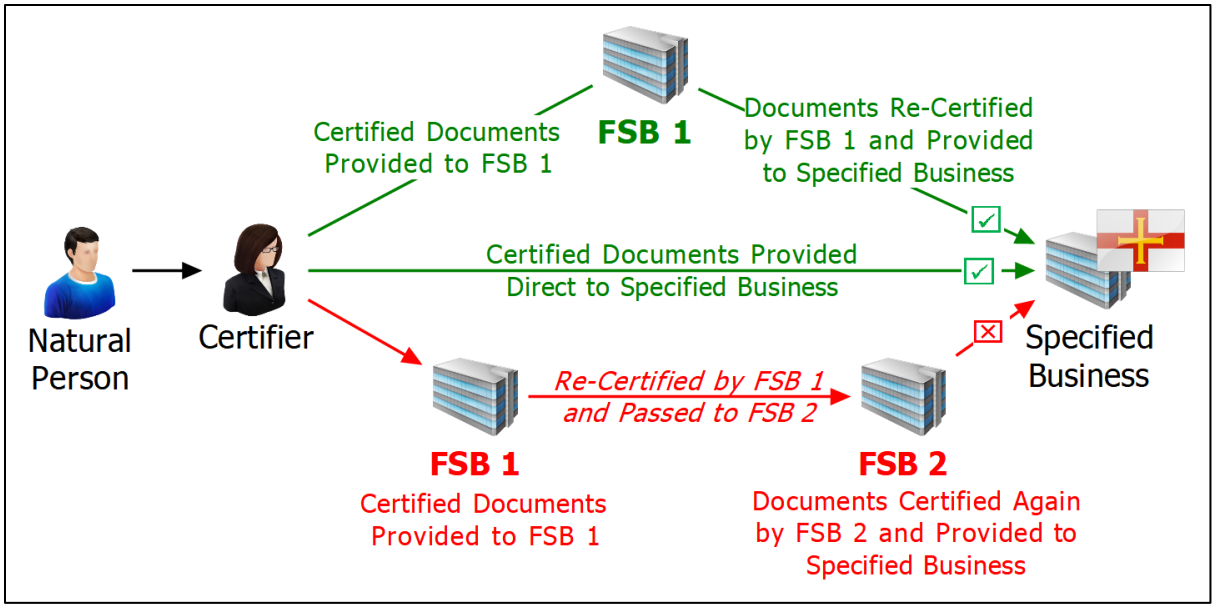


Fig. 3, Chains of Certification

34. Where the firm accepts copies of certified copy *identification data*, the following criteria must be met:

    (a) the copy *identification data* has been provided by an *Appendix C business*;
    (b) the *Appendix C business* has confirmed that the copy provided is a true copy of the *identification data* which it holds;
    (c) the *Appendix C business* has seen the original *identification data* that it has copied to the firm, or the *identification data* that has been copied to the firm was provided to the *Appendix C business* by a suitable certifier, and in the case of the latter, the firm is *satisfied* that the individual who certified the *identification data* accepted by the *Appendix C business* which it is copying to the firm would qualify as a suitable certifier under the firm's policies and procedures; and
    (d) where the *identification data* copied by the *Appendix C business* to the firm relates to the verification of a natural person's identity, the firm is *satisfied* that the copy *identification data* provides evidence that the natural person is who he or she is said to be.

35. For the avoidance of doubt this Section does not apply in respect of *business relationships* or *occasional transactions* falling within the introduced business provisions of Chapter 10 of this *Handbook* or where the firm acquires a business or block of *customers* in accordance with Paragraph 4.47. of this *Handbook*. In such circumstances, the firm places reliance upon a third party to have applied *CDD* measures to a *customer*, *beneficial owner* or other *key principal* in accordance with its own policies, procedures and controls. As such, the firm may accept copies of certified copy documentation either as part of the testing of that third party or through its acquisition of a block of *customers*.

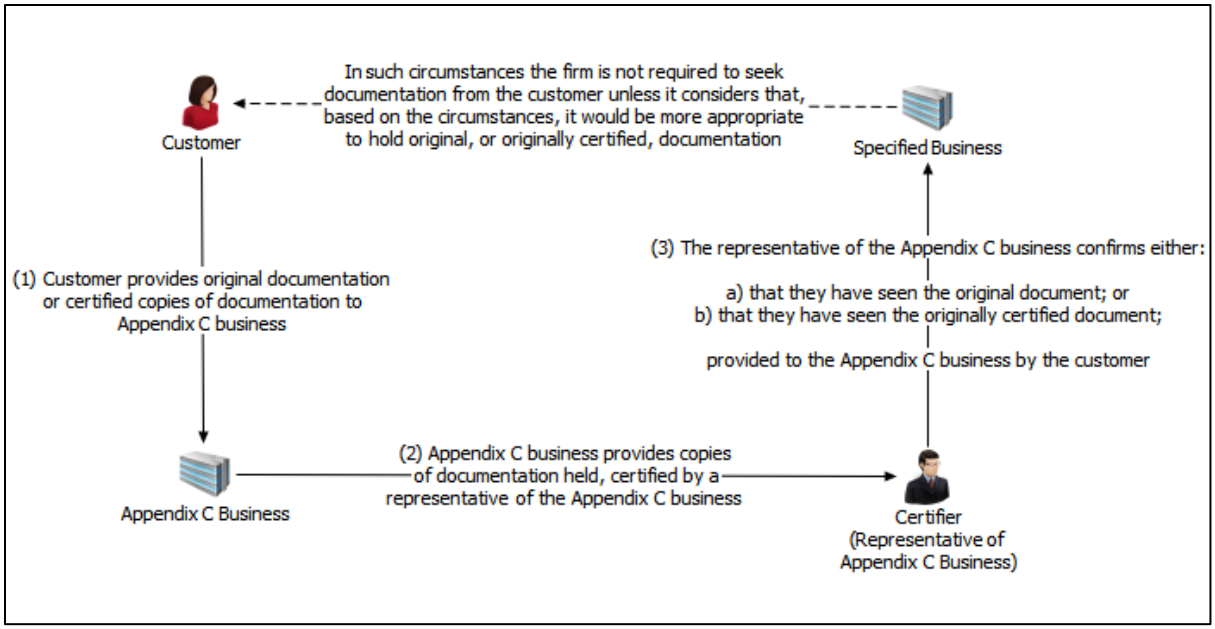


Fig. 4, Flow of Copy Certified Documentation

Chapter 7
Legal Persons and Legal Arrangements

Contents of this Chapter

7.1. Introduction

1. The purpose of this Chapter is to set out the information to be obtained, as a minimum, for a *legal person* or *legal arrangement* which acts as a *key principal* in one or more of the following capacities within a *business relationship* or *occasional transaction* as set out in Paragraph 4(3) of *Schedule 3*:

   (a) the *customer*;
   (b) the *beneficial owner* of the *customer*;
   (c) a *legal person* or *legal arrangement* purporting to act on behalf of the *customer*; or
   (d) a *legal person* or *legal arrangement* on behalf of which the *customer* is acting.

2. The identification and verification requirements in respect of *legal persons* and *legal arrangements* are different from those for natural persons. While a *legal person* or *legal arrangement* has a legal status which can be verified, each *business relationship* or *occasional transaction* involving a *legal person* or *legal arrangement* will also contain a number of associated natural persons, for example, as *beneficial owners*. This Chapter should therefore be read in conjunction with Chapters 4 and 5 which set out the *CDD* measures to be applied to natural persons acting for or on behalf of, or otherwise associated with, a *customer* which is a *legal person* or *legal arrangement*.

3. *Legal person* refers to any entity, other than a natural person, which is treated as a person for limited legal purposes, i.e. it can sue and be sued, it can own property and it can enter into contracts in its own right. This can include companies, other bodies corporate, *foundations*, anstalts, associations, or other similar entities which are not *legal arrangements*.

4. *Legal arrangements* do not have separate legal personality and therefore form *business relationships* through their trustees (or equivalent). With regard to trusts, it is the trustee of the trust who will enter into a *business relationship* or *occasional transaction* on behalf of the trust and should be considered, along with the trust, as the firm's *customer*.

5. There are a wide variety of trusts and other similar arrangements, ranging from large, nationally and internationally active organisations subject to a high degree of public scrutiny and transparency, through to trusts set up under testamentary arrangements and trusts established for wealth management purposes.

6. The firm should be alive to, and take measures to prevent, the misuse of *legal persons* and *legal arrangements* for *ML*, *TF* and *PF*. It is imperative that when compiling a *relationship risk assessment*, the firm considers the breadth of *ML*, *TF* and *PF risks* that the differing size, scale, activity and structure of the *legal person* or *legal arrangement* could pose. Less transparent and/or more complex structures present higher *risks* which could require additional information or research to determine an appropriate *risk* classification.

7. Based on the outcome of its *relationship risk assessment*, the firm must consider how the *customer* and any other *legal persons* or *legal arrangements* falling within the requirements of Paragraph 4(3)(a)-(d) of *Schedule 3* are to be identified and the *identification data* in respect of those *legal persons* or *legal arrangements* which must be obtained to verify that identity, including *ECDD* measures and/or *enhanced measures* where necessary.

8. Where the firm acts as resident agent for a *legal person* established in *the Bailiwick*, it is also subject to *the Beneficial Ownership Law* and *the Beneficial Ownership Regulations* and the reporting requirements contained therein.

Beneficial Ownership of Legal Persons (Guernsey) Law, 2017
Beneficial Ownership (Definition) Regulations, 2017

7.2. Transparency of Beneficial Ownership

9. It is crucial that the firm has a full picture of its *customer*, including those natural persons with ownership or control over the *customer's* affairs. This is important so as to identify, firstly the various legal obligations that fall due within *the Bailiwick* and beyond and, secondly, whether the *legal person* or *legal arrangement* is being abused for criminal purposes. As financial crime legislation, including tax legislation, becomes ever more sophisticated, so too do the ways in which a person may structure his, her or its affairs in order to mask the true beneficial ownership.

10. When applying *CDD* measures in relation to *customers* that are *legal persons* or *legal arrangements*, in accordance with Paragraph 4(3)(c) of *Schedule 3* the firm shall identify and take reasonable measures to verify the identity of the *beneficial owner* of the *legal person* or *legal arrangement*.

11. The definition of *beneficial owner* in the context of *legal persons* is to be distinguished from the concepts of legal ownership and control. On one hand, legal ownership means the natural or *legal person(s)* who, according to applicable law, own the *legal person*. On the other hand, control refers to the ability to make relevant decisions within the *legal person*, for example, by owning a controlling block of shares.

12. An essential element of the definition of *beneficial owner* is that it extends beyond legal ownership and control and focusses on ultimate (actual) ownership and control. In other words, the definition identifies the natural (not legal) persons who actually own and take advantage of the capital or assets of the *legal person*, as well as those who really exert effective control over it (whether or not they occupy formal positions within that *legal person*), rather than just the natural or legal persons who are legally (on paper) entitled to do so.

13. In the context of a trust, beneficial ownership includes both the natural persons receiving benefit from the trust (for example, a beneficiary, those in a class of beneficiaries or any other person who benefits from the trust) as well as those connected with, or having control over, the trust's affairs, including the *settlor(s)*, trustee(s), *protector(s)* and enforcer(s).

14. Paragraph 4(3)(c) of *Schedule 3* also requires that, in the case of a *business relationship* or *occasional transaction* within which the *customer* is a *legal person* or *legal arrangement*, that the firm shall take measures to understand the nature of the *customer*'s business and its ownership and control structure.

15. When taking measures to understand the ownership and control structure of a *customer* in accordance with Paragraph 4(3)(c) of *Schedule 3*, it is not necessary to verify the identity of every *legal person* or *legal arrangement* within a structure. However, the firm must take reasonable measures to gather sufficient information on the identity of any intermediate entities to allow it to identify those natural persons falling within the definition of *beneficial owner* and to identify whether any intermediate entity has issued *bearer shares* or *bearer warrants*.

16. Further detail is provided within this Chapter in relation to identifying the *beneficial owner* in the particular types of *legal persons* and *legal arrangements* with which the firm could enter a *business relationship* or undertake an *occasional transaction*.

17. When identifying, and taking reasonable measures to verify the identity of, the *beneficial owner* of a *legal person* or *legal arrangement* as required by the sections of this Chapter, the firm must act in accordance with the identification and verification requirements of *Schedule 3* and this *Handbook* for natural persons, *legal persons* and *legal arrangements*.

18. Where a *key principal* is a *legal person* or *legal arrangement* authorised or registered by *the Commission* as a CIS under *the POI Law*, the *CDD* measures to be applied to that *legal person* or *legal arrangement* are set out in Section 9.5. of this *Handbook*.

19. Where a *business relationship* or *occasional transaction* involving a *legal person* or *legal arrangement* (taking into account the *beneficial owner(s)* of such) presents a high *risk* and/or requires the application of *enhanced measures*, the firm should refer to the obligations set out within Chapter 8 of this *Handbook*.

7.3. Measures to Prevent the Misuse of Nominee Shareholders and Nominee Directors

20. The use of *nominee shareholders* and *nominee directors* can provide a means to obscure ultimate ownership and control of a *legal person* or *legal arrangement*. To minimise the risk to the firm of providing products or services to a *customer* using such arrangements, it is critical that legal and beneficial ownership is recorded thoroughly and that appropriate steps are taken to establish the true identity of those persons with ultimate ownership and control of a *customer*.

21. The firm must have appropriate and effective procedures to prevent the misuse of *nominee shareholders* and *nominee directors*. These must include a requirement to consider whether a *legal person* has *nominee shareholders* and/or *nominee directors* and the means to identify, and take reasonable measures to verify the identity of, any natural person who ultimately controls a *legal person* or *legal arrangement* for which *nominee shareholders* and/or *nominee directors* are identified in the ownership and control structure.

22. Where the firm identifies that the *customer* is a *legal person* with *nominee shareholders*, or is owned by a *legal person* with *nominee shareholders*, in accordance with Paragraph 5(2)(d) of *Schedule 3* it shall apply *enhanced measures* as set out in Section 8.12. of this *Handbook*, regardless of the *risk* rating attributed to the *business relationship* or *occasional transaction*.

23. For the purposes of identifying the *beneficial owner* of a *legal person* or *legal arrangement*, a *nominee shareholder* or *nominee director* would not be considered to have ultimate ownership or control of the *customer*. The firm must therefore look through the *nominee shareholder* or *nominee director* and identify from whom instructions are being taken by a *nominee director* and for whom shares or interests are held by the *nominee shareholder*.

7.3.1. Nominee Shareholders

24. A *nominee shareholder* is a natural or *legal person* recorded in the share register as the shareholder of a *legal person* who holds the shares or interest in that *legal person* on behalf of another. The identity of the true *beneficial owner(s)* is not disclosed on the register. In this instance the *nominee shareholder* cannot be considered the *beneficial owner*.

25. *Nominee shareholders* can be used to hide or obscure the beneficial ownership of a *legal person*, for example, a natural person may indirectly hold a majority interest in a *legal person* through the use of *nominee shareholders* who each hold a minimal interest and thereby obscure the identity of the natural person who actually holds effective control.

26. To mitigate the increased *risk* posed by *nominee shareholders*, the provision of, or acting as, a *nominee shareholder* in *the Bailiwick* by way of business is an activity which requires licensing under *the Fiduciaries Law* and is therefore subject to the requirements of *Schedule 3* and the *Commission Rules* in this *Handbook*. A similar approach is adopted in a number of other jurisdictions, such as the Bailiwick of Jersey and the Isle of Man. While this factor may reduce the inherent *risk* with *nominee shareholders*, it does not provide for the disapplication of *Commission Rule* 7.23.

7.3.2. Nominee Directors

27. A *nominee director* is a natural or *legal person* who acts on behalf of another. A *nominee director* therefore cannot be considered to be the *beneficial owner* on the basis that they are being used by someone else who can ultimately exercise effective control over that *legal person*.

28. Steps have been taken within *the Bailiwick* to counter the risk of natural or *legal persons* acting as *nominee director* by requiring that those who provide or act as director be licensed under *the Fiduciaries Law* and therefore subject to the requirements of *Schedule 3* and the *Commission Rules* in this *Handbook*. However, the firm should remain alert in respect of *legal persons* from all jurisdictions for indications that a director might be acting on the instructions of another person.

29. Factors which may indicate that a person is acting as a director on behalf of an undisclosed party could include:

(a) where the individual's credentials, such as their occupation, are inconsistent with the *legal person's* activity and purpose;
(b) where the individual holds other unrelated board appointments; or
(c) there are indications in communications the firm has with the *legal person* that the director could be taking instructions from another person whose relationship with that *legal person* is unclear.

7.4. Legal Persons

7.4.1. Identifying and Verifying the Identity of Legal Persons

30. Where a *legal person* is a *key principal* to a *business relationship* or *occasional transaction*, the firm must identify and verify the identity of that *legal person* (or take reasonable measures to do so in accordance with Paragraph 4(3)(c) or (d) of *Schedule 3*), including as a minimum:

(a) the name of the *legal person*, including any trading names;
(b) any official identification number;
(c) the legal form and law to which the *legal person* is subject and the powers that regulate and bind the *legal person*;
(d) the date and country/territory of incorporation/registration/establishment (as applicable);
(e) the registered office address and principal place of business (where different from the registered office); and
(f) the names of the natural persons having a senior management position (for example, the directors (or equivalent)) in the *legal person*.

31. The following non-exhaustive list provides examples of *documents* considered suitable to verify one or more aspect of the identity of a *legal person*:

(a) a copy of the Certificate of Incorporation (or equivalent);
(b) a copy of the Memorandum and Articles of Incorporation (or equivalent);
(c) a copy of the latest audited financial statements;
(d) a copy of the latest annual return;
(e) a copy of the register of directors;
(f) a copy of the register of shareholders;
(g) a company registry search including confirmation that the *legal person* has not been, and is not in the process of being, dissolved, struck off, wound up or terminated;
(h) independent information sources, including electronic sources;
(i) a copy of the board resolution authorising the opening of any *account* and recording the *account* signatories; and/or

(j) a personal visit to the principal place of business.

32. Where the *documents* obtained are copies of the originals, the firm should refer to the requirements of Section 6.6. of this *Handbook*.

33. In seeking to identify and verify the names of the natural persons having a senior management position in accordance with *Commission Rule* 7.30.(f), the firm should obtain information on the identity of the directors of the *legal person* or equivalent positions who impose binding obligations upon a *legal person*, including authorised signatories, and verify that those positions are held.

34. Where one or more directors (or equivalent) or authorised signatories act for or on behalf of the *legal person* in a *business relationship* or *occasional transaction* with the firm, those persons should be identified, and their identity verified, in accordance with Section 4.3.2 of this *Handbook*. Where this is through a corporate director of a *legal person*, the firm should identify and verify the names of the directors of the corporate director and identify and verify the natural persons who will be representing the corporate director acting for the *legal person*. Where an individual authorised to act on behalf of the *legal person* is acting in the course of employment with a *transparent legal person* it is not necessary to identify and verify the identity of the person, providing that confirmation has been received from the *transparent legal person* that the individual is authorised to act.

35. It may be the case that not all directors (or equivalent) of a *legal person* will be acting for it within the relationship with the firm. The firm will have to identify and verify that the individual holds that position, but if that person does not act for the *legal person* in an executive capacity in the relationship with the firm, the firm does not need to identify and verify the identity of that director.

7.4.2. Identifying and Verifying the Identity of the Beneficial Owners of Legal Persons

36. Paragraph 22(2) of *Schedule 3* defines *beneficial owner* for the purposes of identification and verification as being:

Step 1. the natural person who ultimately controls the *legal person* through ownership; or, if no such person exists or can be identified,
Step 2. the natural person who ultimately controls the *legal person* through other means; or, if no such person exists or can be identified,
Step 3. the natural person who holds the position of a senior managing official of the *legal person*.

37. The steps set out in Paragraph 7.36. above are not alternative options. Establishing the beneficial ownership of a *legal person* is a cascading process, beginning with Step 1. If no *beneficial owner* is identified at Step 1 or there are doubts as to the accuracy of the natural person identified as the *beneficial owner*, the firm should move to Step 2 and where no natural person is identified under either Steps 1 and/or 2, ultimately Step 3.

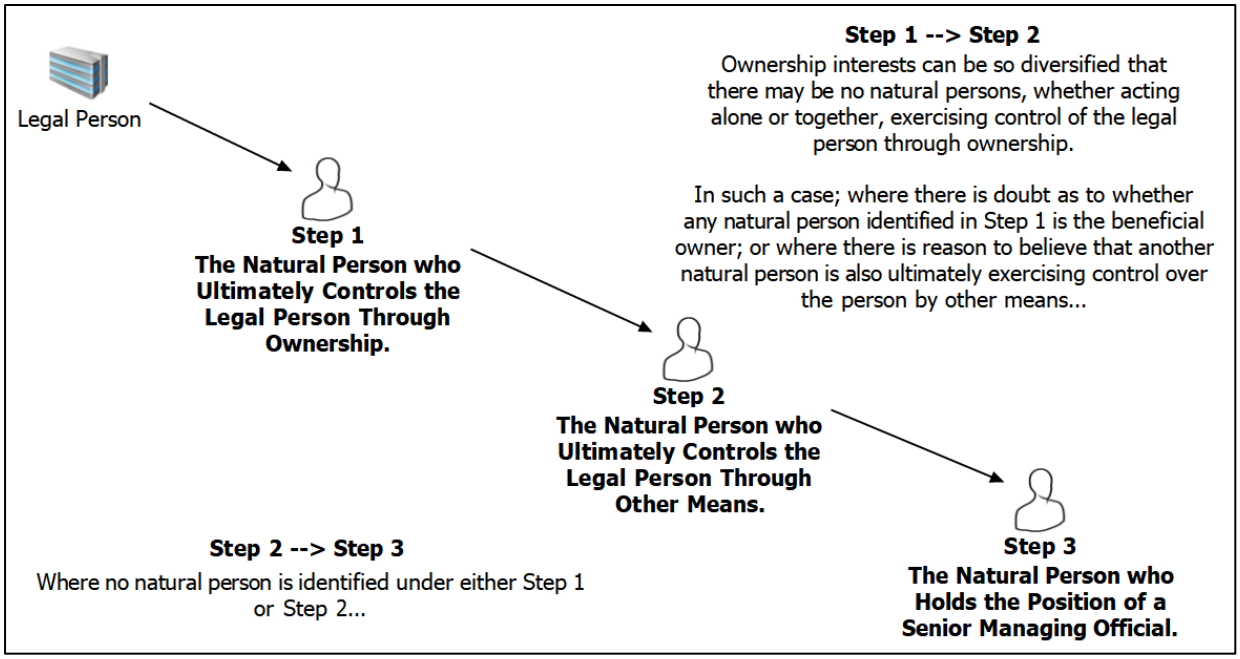


Fig. 5 – Three Step Test of Beneficial Ownership

38. For the purposes of Step 1, in accordance with Paragraph 22(6) of *Schedule 3*, a person has control of a *legal person* through ownership if that person holds, directly or indirectly, any of the following:

    (a) if the *legal person* is a company,

        (i) more than 25% of the shares in the company,
        (ii) more than 25% of the *voting rights* in the company, or
        (iii) the right to appoint or remove directors holding a majority of *voting rights* on all or substantially all matters at meetings of the board,

    (b) if the *legal person* is any other form of *legal person* other than a *foundation*,

        (i) more than 25% of the shares in the *legal person* or an interest equivalent to a shareholding of more than 25%, including but not limited to an entitlement to more than 25% of the assets of the *legal person* in the event of its winding up or dissolution,
        (ii) more than 25% of the *voting rights* in the conduct or management of the *legal person*, or
        (iii) the right to appoint or remove a majority of the managing officials of the *legal person* holding a majority of *voting rights* on all or substantially all matters at meetings of the *legal person* that are equivalent to board meetings.

39. For the purposes of Paragraph 7.38. above, in accordance with Paragraph 22(6) of *Schedule 3* holding more than 25% of the shares in a company means holding a right or rights to share in more than 25% of the capital or, as the case may be, the profits of the company.

40. It should be noted that, in accordance with Paragraph 22(7) of *Schedule 3*, a person holds shares or rights for the purposes of Paragraphs 7.38. and 7.39. above if:

    (a) those shares or rights constitute *joint interests*;
    (b) those shares or rights are held under a *joint arrangement*;
    (c) those shares or rights are held on behalf of that person by a nominee;

(d) in the case of rights, that person controls their exercise;
(e) in the case of rights only exercisable in certain circumstances, those rights are to be taken into account; or
(f) in the case of rights attached to shares held by way of security provided by a person, the rights are still exercisable by that person.

41. In accordance with Paragraph 22(11) of *Schedule 3*, for the purposes of *Schedule 3* and this *Handbook*, references (however expressed) to,

(a) a person controlling the exercise of a right,
(b) taking rights into account, or
(c) rights being exercisable by a person,

shall be construed consistently with Paragraphs 10(2), 11 and 12(a)-(b) of *the Beneficial Ownership Regulations* respectively.

42. It should be borne in mind that a natural person could also indirectly hold an ownership interest in a *legal person*. This situation could arise where, for example, a person holds their ownership in the *legal person* through a *legal arrangement*. In all cases it is important to note that, if a natural person is identified within an ownership structure in more than one way, the value of each of that person's holdings will be looked at cumulatively in order to assess that person's overall holding.

43. In accordance with Paragraph 22(4) of *Schedule 3*, in any case where a trust or other *legal arrangement* controls a *legal person* through ownership, the *beneficial owners* of that *legal person* are the *beneficial owners* of that trust or other *legal arrangement* as detailed in Section 7.10. of this Chapter.

44. In accordance with Paragraph 22(5) of *Schedule 3*, in any case where a *transparent legal person* has control of a *legal person* through ownership ("the controlled *legal person*"), that *transparent legal person* shall be treated as a natural person for the purposes of *Schedule 3* and *this Handbook*, and therefore (for the avoidance of doubt) as the *beneficial owner* of the controlled *legal person.*

45. A *transparent legal person* is defined in Paragraph 22(10) of *Schedule 3* as being:

(a) a company that is listed on a recognised stock exchange within the meaning of *the Beneficial Ownership Regulations*, or a majority owned subsidiary of such a company;
(b) a States trading company within the meaning of the States Trading Companies (Bailiwick of Guernsey) Law, 2001;
(c) a *legal person* controlled by the States of Alderney through ownership within the meaning of the Beneficial Ownership (Alderney) (Definition) Regulations, 2017 (or any successor regulations made under Section 25 of the Beneficial Ownership of Legal Persons (Alderney) Law, 2017; or
(d) a regulated person within the meaning of Section 41(2) of *the Beneficial Ownership Law*, being a person who:

(i) holds or is deemed to hold a licence granted to it by *the Commission* under *the Regulatory Laws*; or
(ii) carries on a *PB* for the purposes of *the PB Law.*

46. Ownership interests can be so diversified that there may be no natural person, whether acting alone or together with another, who ultimately controls a *legal person* through ownership. Where

this is the case, the firm should move to Step 2 and seek to identify and verify the identity of the natural person who ultimately controls the *legal person* through other means.

47. As set out in Paragraph 22(3) of *Schedule 3*, there may also be a case where:

(a) the natural person who controls the *legal person* through ownership has been identified in accordance with Step 1,
(b) there are reasonable grounds to believe that the *legal person* is also ultimately controlled by another natural person through other means, and
(c) that other natural person can be identified.

48. In the above situation, or where there is doubt as to whether a natural person identified in Step 1 is the *beneficial owner*, the *beneficial owners* in relation to the *legal person* are the person with the controlling ownership interest and the other natural person believed to be ultimately exercising control over the *legal person* by other means (i.e. the persons identified within both Steps 1 and 2).

49. Whether or not this situation arises will depend on the specific factors of each case. By way of example, it may arise where the natural person with the controlling ownership interest is dominated by another because of a familial, employment, historical or contractual association, or where another natural person holds certain powers in relation to the *legal person* which are being or are likely to be used in practice to affect decisions taken by the natural person with the controlling ownership interest.

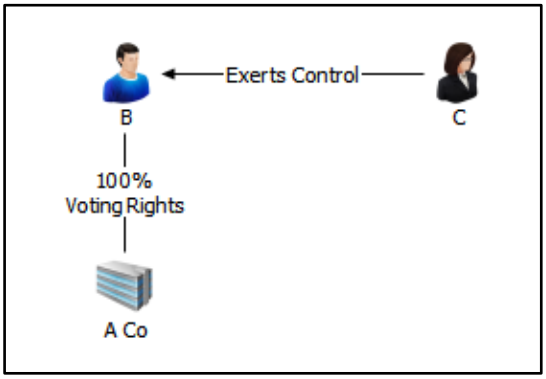


Fig. 6 – Control Through Other Means

In this example, A Co is a *legal person* which is the *customer* to a *business relationship* with the firm. B holds 100% of the *voting rights* in A Co.

Although B works as a gardener with no other source of income, A Co has considerable assets. B's employer, C, is a well-known international businesswoman who is famous for her desire for privacy, in particular about the location of her assets.

The firm therefore has reason to believe that, although B controls A Co through ownership, C is also ultimately controlling A Co through other means, i.e. her relationship with B, and both B and C are to be treated as *beneficial owners* of A Co.

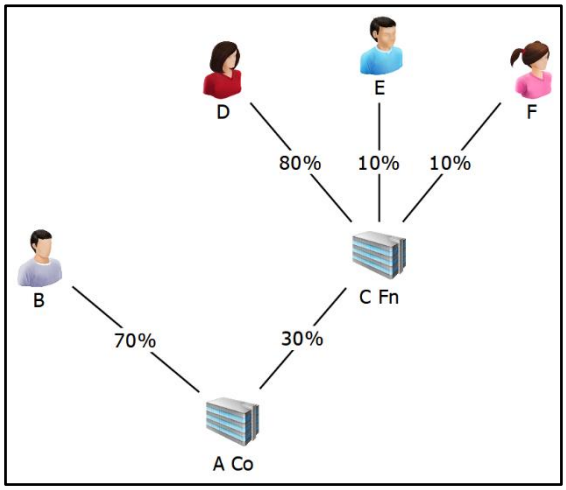
50. For the purposes of Steps 1 and 2 in Paragraph 7.36., a natural person holds a share or right directly when that share or right is held in that person's own name. This may be held by the natural person alone or jointly with another. Direct holdings will generally be recorded in the constitutional documents of a *legal person* (for example, a register of shares). However, the firm should be mindful that the information in the constitutional documents may not be definitive (for example, there may be persons controlling that *legal person* through other means as in Fig. 6 above).

51. Conversely, a natural person holds a share or right indirectly where the ownership structure of a *legal person* involves one or more other entities, i.e. a chain of ownership. Where this is the case the firm should look through the chain of ownership to establish the ownership interests in each entity to ensure that all natural persons with an indirect holding of more than 25% of the shares or rights in the *legal person* are identified. The ownership interests within a chain that need to be quantified are most likely to be shares or rights (or possibly vested beneficial interests in the case of a *foundation*). However, the relevance of an ownership interest will depend on the particular

features of the intermediate entities, some of which may be established under the laws of other jurisdictions.

52. An indirect holding within a chain of ownership may arise in one of two ways. The first is when an entity holds more than 25% of the shares or rights in the *legal person* and an individual has a majority stake (i.e. a greater than 50% shareholding or similar) in that entity so can control those shares or rights. The majority stake may be held directly, but it may also be held through a chain of ownership with the individual holding a majority stake in each intervening entity. The second is where the overall value of an individual's holding in shares or rights in the *legal person*, when quantified back through the ownership chain, amounts to more than 25%. An individual who has indirect ownership in either or both of these ways is a *beneficial owner* of the *legal person*.

Fig. 7 – Direct Holding vs. Indirect Holding



In this example, A Co is a *legal person* which is the *customer* to an *occasional transaction* with the firm. B holds 70% of the shares in A Co through a direct holding and is therefore a *beneficial owner* of A Co. The remaining 30% of the shares are held by C Fn, a foreign *foundation*.

D holds 80% of the shares in C Fn so has an indirect holding in A Co quantified at 24% overall (i.e. 80% of 30%). This means D does not have an overall holding in A Co of more than 25% under the quantification test, but does hold a majority stake in an entity which holds more than 25% of the *voting rights* in A Co, therefore D is a *beneficial owner* in A Co.

E and F each hold 10% of the shares in C Fn, so each has an indirect holding in the shares of A Co of 3% overall (i.e. 10% of 30%). As they have neither an overall holding in A Co of more than 25% under the quantification test, nor a majority stake in an entity which holds more than 25% of the *voting rights* in A Co, they are not *beneficial owners* of A Co.

53. Finally, where no natural person is identified under either of Step 1 or Step 2 in Paragraph 7.36., in accordance with Step 3 the firm would identify and take reasonable measures to verify the identity of the natural person who holds the position of a senior managing official of the *legal person*.

54. The senior managing official could be the natural person responsible for strategic decisions that fundamentally affect the business or general direction of the *legal person* (for example, a director (or equivalent)) or the natural person exercising executive control over the daily or regular affairs of the *legal person* through a senior management position (for example, the chief executive officer or chief finance officer). In both cases, this would not normally include a person who does not have executive functions, such as a non-executive director.

55. In situations where there is more than one official of a *legal person* with strategic decision making powers and none is senior to the others, for the purposes of *Schedule 3* and this *Handbook*, all should be treated as senior managing officials.

56. In the case of partnerships; associations; clubs; societies; charities; church bodies; institutes; mutual and friendly societies; and co-operative and provident societies, the senior managing officials will often include members of the governing body or committee plus executives. In the case of *foundations*, this will include members of the governing council and any supervisors.

7.5. Legal Bodies Listed on a Recognised Stock Exchange

57. In accordance with Paragraph 4(4) of *Schedule 3*, the firm shall not be required to identify any shareholder or *beneficial owner* in relation to:

(a) a *customer*, and
(b) a person which ultimately controls a *customer*,

that is a company listed on a recognised stock exchange within the meaning of *the Beneficial Ownership Regulations*, or a majority owned subsidiary of such a company.

Beneficial Ownership (Definition) Regulations, 2017, as amended

58. In order for the firm to consider the company as the principal to be identified, it must obtain *documentation* which confirms that the company is listed on a recognised stock exchange.

59. For the purposes of Paragraph 4(4) of *Schedule 3* and *Commission Rule* 7.58. above, in accordance with *the Beneficial Ownership Regulations* the following are deemed to be recognised stock exchanges:

(a) any regulated market within the meaning of the European Directive on Markets in Financial Instruments 2004/39/EU;
(b) the International Stock Exchange Authority Limited;
(e) the Australian Securities Exchange;
(f) the New York Stock Exchange;
(g) the National Association of Securities Dealers Automated Quotation System;
(h) the Cayman Islands Stock Exchange;
(i) the Bermuda Stock Exchange;
(j) the Hong Kong Stock Exchange;
(k) the Johannesburg Stock Exchange;
(l) the SIX Swiss Exchange;
(m) the London Stock Exchange Main Market, including the Alternative Investment Market and the Specialist Fund Segment;
(n) the Cboe Europe Equities Regulated Market; and
(o) Aquis Stock Exchange Limited.

EU Markets in Financial Instruments Directive 2004

7.6. Protected Cell Companies

60. A protected cell company ("PCC") is a single legal entity with one board of directors and one set of memorandum and articles of incorporation. A PCC can create an unlimited number of protected cells ("PCs"), the assets and liabilities of which are separate from those of the PCC (with the assets of the latter referred to as "non-cellular" or "core"). Importantly, the PCs are not separate legal entities and therefore cannot transact as such.

61. A PCC can be a newly incorporated entity or alternatively an existing company can be converted to a PCC. In either case the formation of, or conversion to, a PCC within *the Bailiwick* requires, under the Companies (Guernsey) Law, 2008 as amended, the prior written consent of *the Commission*.

62. A PCC may create any number of PCs, the assets and liabilities of which are segregated from the non-cellular assets of the PCC and from the assets and liabilities of other PCs. However, a PC may not own shares in its own PCC or another PC of the same PCC.

63. Where a PCC is a *key principal* to a *business relationship* or *occasional transaction*, the firm must apply *CDD* measures to both the core and the relevant PC(s), including the *beneficial owners* of such, in accordance with the requirements for *legal persons*.

64. Notwithstanding the segregation in respect of the assets and liabilities of the core and PCs as detailed above, for the purposes of identifying and verifying the identity of the *beneficial owner* in accordance with Paragraph 4(3) of *Schedule 3*, the test for control through ownership of a PCC is two-fold and will differ depending on the circumstances of the firm's relationship with the PCC (or a PC thereof):

(a) Where the firm is entering into a *business relationship* or undertaking an *occasional transaction* with a PC (for example, the provision of a *bank account* for a particular PC), the beneficial ownership should be calculated separately in respect of:

(i) the shares or rights in the particular PC; and
(ii) the shares or rights in the core.

(b) Where the firm acts as administrator of the PCC, the beneficial ownership should be calculated in respect of the shares or rights in the PCC as a whole in the same way as with any other *legal person* and ignoring any segregation (i.e. including any shares or rights held in the core, as well as all PCs).

65. For the purposes of Paragraph 7.64.(b), a natural person's direct or indirect holding of shares or rights in a PCC is therefore calculated by including all shares or rights that the person holds in the PCC, whether those shares or rights form part of the core or are held within one or more PCs. The effect of this is that a person cannot try to conceal his or her beneficial ownership of a PCC by dividing shares among different PCs.

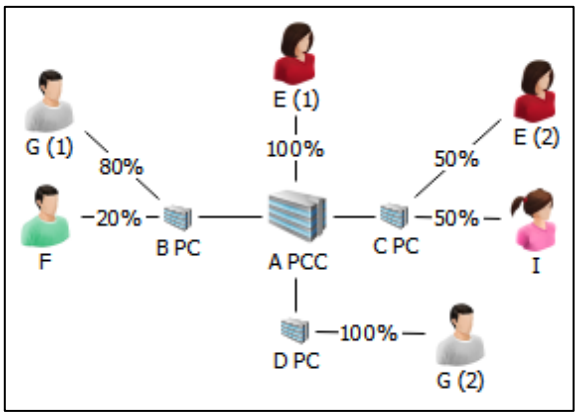


Fig. 8 – Beneficial Ownership of PCCs

In this example, A PCC is a PCC with three cells. E holds all of the shares in the core and 50% of the shares in C PC. E is therefore a *beneficial owner* of C PC, and holds 37% of all shares, making her a *beneficial owner* of A PCC.

Likewise, G holds 100% of the shares in D PC and 80% of the shares in B PC. G is therefore a *beneficial owner* of D PC and B PC, and holds 45% of the total shares making him a *beneficial owner* of A PCC.

I holds 50% of the shares in C PC and 12.5% of the shares in A PCC. I is therefore a *beneficial owner* of C PC, but not A PCC. Finally, F holds 20% of the shares in B PC and 5% of the total shares in the PCC. F is neither a *beneficial owner* of B PC or the A PCC structure.

66. The *CDD* measures to be applied to a PCC authorised or registered by *the Commission* as a CIS under Section 8 of *the POI Law* where it acts as a *key principal* to a *business relationship* or *occasional transaction* are set out in Section 9.5. of this *Handbook.*

67. The *CDD* measures for PCCs which are licensed under the Insurance Business (Bailiwick of Guernsey) Law, 2002 as amended ("*the IB Law*") and where the *beneficial owner* of the relevant PC or PCC is a business which is listed on a recognised stock exchange within the meaning of *the Beneficial Ownership Regulations* (or by a majority owned subsidiary of such a listed business) are the same as those set out in Section 7.5. of this *Handbook.*

7.7. Incorporated Cell Companies

68. An incorporated cell company ("ICC") is structured similarly to a PCC with a non-cellular core and an unlimited number of cells ("ICs"). However, in contrast, the ICs of an ICC are separately incorporated and are therefore distinct legal entities with their own memorandum and articles of incorporation and boards of directors.

69. It is of note that the boards of the ICC and the boards of the ICs must be identically composed, so any director of an ICC must also be a director of each of its ICs.

70. Similar to a PCC, the assets and liabilities of each IC are segregated from the assets and liabilities of the ICC and from the assets and liabilities of the other ICs. While an IC can hold its own assets, those assets cannot include shares in its own ICC.

71. As a result of each IC having separate legal personality, the ICs have the ability to contract with third parties and with other ICs in their own right. An IC must therefore contract in respect of its own affairs and the ICC has no power to enter into transactions on behalf of any of its ICs. Each IC can also have distinct *beneficial owners*.

72. Where an ICC or IC is a *key principal* to a *business relationship* or *occasional transaction*, the firm must apply *CDD* measures to the relevant ICC or IC, and to the *beneficial owners* thereof, in accordance with the requirements for *legal persons*.

73. The *CDD* measures to be applied to an ICC or IC authorised or registered by *the Commission* as a CIS under Section 8 of *the POI Law* where it acts as a *key principal* to a *business relationship* or *occasional transaction* are set out in Section 9.5. of this *Handbook*.

74. The *CDD* measures for ICs or ICCs which are licensed under *the IB Law* and where the *beneficial owner* of the relevant IC or ICC is a business which is listed on a recognised stock exchange within the meaning of *the Beneficial Ownership Regulations* (or by a majority owned subsidiary of such a listed business) are the same as those set out in Section 7.5. of this *Handbook.*

7.8. Limited Partnerships and Limited Liability Partnerships

75. An LP is a form of partnership with or without legal personality at the election of the GP. Its members include one or more GP, who has actual authority over the LP, for example to bind the LP in contracts with third parties, and is liable for all debts of the LP, and one or more limited partner who contributes (or agrees to contribute) to the capital of the LP and who (subject to certain provisions) is not liable for the debts of the LP.

76. A Limited Liability Partnership ("LLP") is a body corporate with legal personality separate from that of its members and is therefore liable for its own debts. As a consequence of this legal personality, LLPs established within *the Bailiwick* must be registered and therefore public records exist similar to those for *legal persons*. With regard to the members of an LLP, there must be at least two who, unless otherwise stipulated within the members' agreement, may take part in the conduct and management of the LLP and are entitled to share equally in the profits of the LLP.

77. Where an LP or LLP is a *key principal* to a *business relationship* or *occasional transaction*, the firm must identify, and verify the identity of, that LP/LLP (or take reasonable measures to do so in accordance with Paragraph 4(3)(c) or (d) of *Schedule 3*), as set out in Section 7.4. above.

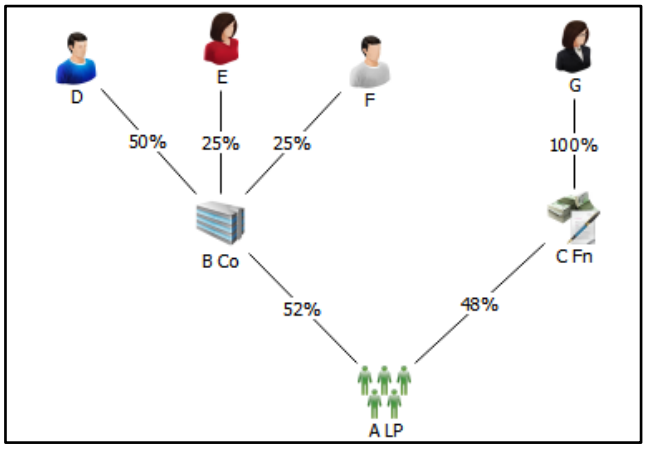
78. The following non-exhaustive list provides examples of *documents* considered suitable to verify one or more aspect of the identity of the LP/LLP in accordance with *Commission Rule* 7.77.:

(a) a copy of the LP/LLP agreement;
(b) a copy of the certificate of registration/establishment;
(c) a copy of the register of limited partners;
(d) a copy of the resolution of the GP (in the case of an LP) or members (in the case of an LLP) authorising the opening of any *bank account* and recording the *account* signatories;
(e) a copy of the latest audited financial statements; and/or
(f) information obtained from independent data sources, including electronic sources, for example a search of a register of LPs/LLPs.

79. Where the *documents* obtained are copies of the originals, the firm should refer to the requirements of Section 6.6. of this *Handbook*.

80. When seeking to identify, and verify the identity of, the *beneficial owners* of an LP/LLP, the firm must act in accordance with the requirements for *legal persons* in *Schedule 3* and the *Commission Rules* in Section 7.4.2. of this *Handbook*.

Fig. 9 – Limited Partnership



In this example, A LP is a limited partnership which is the *customer* to a *business relationship* with the firm. 52% of the *voting rights* in A LP are held by B Co, a limited company, with the remaining 48% held by a *foundation*, C Fn.

D holds 50% of the shares in B Co so has an indirect holding in the *voting rights* in A LP of 26% overall (i.e. 50% of 52%). This means D does not hold a majority stake in an entity that holds more than 25% of the *voting rights* in A LP, but has an overall holding in the *voting rights* in A LP under the quantification test of more than 25%. Therefore D is a *beneficial owner* of A LP.

E and F each hold 25% of the shares in B Co so both have an indirect holding in the *voting rights* in A LP of 13% overall (i.e. 25% of 52%). As they have neither an overall holding in the *voting rights* in A LP under the quantification test of more than 25%, nor a majority stake in B Co, an entity which holds more than 25% of the *voting rights* in A LP, they are not *beneficial owners* of A LP.

G has a vested beneficial interest in 100% of the assets of C Fn, so has an indirect holding in the *voting rights* in A LP of 48% overall (i.e. 100% of 48%). This means that G both holds a majority stake in an entity that holds more than 25% of the *voting rights* in A LP and has an overall holding in the *voting rights* in A LP under the quantification test of more than 25%. Therefore, G is a *beneficial owner* of A LP under both tests.

7.9. Foundations

7.9.1. Obligations of Businesses Establishing or Administering Foundations

81. During the course of establishing or administering a *foundation* relationship, the firm must, in order to identify and verify the identity of the *customer* and *beneficial owners*, identify:

(a) the *founder*(s), including the initial *founder(s)* and any persons or *legal arrangements* subsequently endowing the *foundation*;
(b) all councillors;

(c) any guardian(s);
(d) any *beneficial owner*, including any default recipient; and
(e) any other natural person who exercises ultimate effective control over the *foundation*.

7.9.2. Obligations when Dealing with Foundations

82. Where a *foundation* is a *key principal* to a *business relationship* or *occasional transaction*, the firm must:

(a) identify and verify the identity of the *foundation* (or take reasonable measures to do so in accordance with Paragraph 4(3)(c) or (d) of *Schedule 3)*, including without limitation:

(i) the full name;
(ii) the legal status of the *foundation* and the powers that regulate and bind the *foundation*;
(iii) any official identification number (for example, a registered number, tax identification number or registered charity or NPO number, where relevant);
(iv) the date and country or territory of establishment/registration; and
(v) the registered office address and principal place of operation/administration (where different from the registered office);

(b) identify and verify the identity of any registered agent of the *foundation*, other than where the agent is a *transparent legal person*;
(c) identify the following:

(i) the *founder*(s), including the initial *founder(s)* and any persons or *legal arrangements* subsequently endowing the *foundation*;
(ii) all councillors;
(iii) any guardian(s);
(iv) any *beneficial owner*, including any default recipient; and
(v) any other natural person who exercises ultimate effective control over the *foundation*; and

(d) understand the nature of the *foundation*'s business and its ownership and control structure and the purpose and intended nature of the *business relationship* or *occasional transaction*.

83. The following non-exhaustive list provides examples of *documents* considered suitable to verify one or more aspect of the identity of a *foundation*:

(a) a copy of the Certificate of Registration;
(b) a registry search, if applicable, including confirmation that the *foundation* has not been, and is not in the process of being, dissolved, struck off, wound up or terminated;
(c) a copy of the latest audited financial statements;
(d) a copy of the Charter; and/or
(e) a copy of the Council Resolution authorising the opening of the *account* and recording *account* signatories.

84. Where the *documents* obtained are copies of the originals, the firm should refer to the requirements of Section 6.6. of this *Handbook*.

85. Verification of the identity of the *beneficial owners* of a *foundation* must be undertaken either by the firm itself or, provided that the *Commission Rules* in Chapter 10 of this *Handbook* are met, by requesting the registered agent, where one has been appointed, to provide the relevant information on the identity of such parties by way of a certificate or summary sheet.

7.9.3. Verifying the Identity of the Beneficial Owners of Foundations

86. Paragraph 22(6)(c) of *Schedule 3* defines that a person has control of a *foundation* through ownership if that person holds, directly or indirectly, any of the following:

(a) an interest equivalent to a shareholding of more than 25% including but not limited to an entitlement to more than 25% of the assets of the *foundation* in the event of its winding up or dissolution;
(b) more than 25% of the *voting rights* in the conduct or management of the *foundation*;
(c) the right to appoint or remove a majority of the managing officials of the *foundation* holding a majority of *voting rights* on all or substantially all matters at meetings of the *foundation* that are equivalent to board meetings;
(d) a vested beneficial interest or future entitlement to benefit from more than 25% of the assets of the *foundation*.

87. Other than where a *business relationship* or *occasional transaction* has been assessed as high *risk*, the firm must take reasonable measures to verify the identity of any natural person falling within Paragraph 7.86. above prior to any distribution of *foundation* assets to (or on behalf of) that natural person.

88. Where a *business relationship* has been assessed as being high *risk*, the firm must, where possible, take reasonable measures to verify the identity of any natural person falling within Paragraph 7.86. above at the time that the assessment of *risk* is made. Where it is not possible to do so (for example, because that person has not been born or is disenfranchised) the reasons must be documented and retained on the relevant *customer's* file.

89. The firm must take reasonable measures to verify the identity of those parties identified by *Commission Rule* 7.81. or 7.82. other than the *beneficial owners* (for example, the *founder*(s), *foundation official*(s), councillors, guardian(s) and any other person(s) with ultimate effective control over the *foundation* (including the *beneficial owners* of such entities where they are *legal persons* or *legal arrangements*)) before or during the course of establishing a *business relationship* or before carrying out an *occasional transaction*.

90. Regardless of form, where the firm identifies that a *founder* is acting on behalf of another person, i.e. as a nominee *founder*, the firm must identify and take reasonable measures to verify the identity of the true economic *founder*.

91. With regard to Paragraph 7.86.(d), the persons falling within this category will depend on the specific circumstances of the *foundation*. However, this will generally include individuals who under the terms of the official documents of the *foundation* have a future entitlement to a substantial benefit from the *foundation*. As a matter of practice and policy, this will generally mean an entitlement to a benefit which in the hands of an individual recipient equates to more than 25% of the total assets of the *foundation*. In other words, it is not intended that, where a *foundation's* official documents anticipate the provision of benefits to a potentially large group, (for example, by providing *funds* to supply food to the inhabitants of a flooded village) members of that group should be treated as *beneficial owners*.

7.10. Trusts and Other Legal Arrangements

7.10.1. Obligations of Trustees (or Equivalent)

92. During the course of establishing a trust relationship for which it is to act as trustee, the firm must, in order to identify and verify the identity of the *customer* and *beneficial owners*, identify:

(a) the *settlor*(s), including the initial *settlor(s)* and any persons or *legal arrangements* subsequently settling *funds* into the trust;
(b) any *protector*(s), enforcer(s) and co-trustee(s);
(c) any beneficiary (whether his or her interest under the trust is vested, contingent or discretionary and whether that interest is held directly by that person or as the *beneficial owner* of a *legal person* or a *legal arrangement* that is a beneficiary of the trust), any class of beneficiaries and any other person who is likely to benefit from the trust; and
(d) any other natural person who exercises ultimate effective control over the trust.

93. Where the firm is establishing a *legal arrangement* other than a trust for which it is to act in a position equivalent to that of a trustee, the firm must identify those persons fulfilling positions equivalent to those set out in *Commission Rule* 7.92. above.

94. In identifying any person who is likely to benefit from the trust in accordance with *Commission Rule* 7.92.(c), the firm should seek to establish whether any documentation other than the trust deed, for example, a letter of wishes, identifies persons other than beneficiaries who, in the view of the trustee, are likely to benefit from the trust.

95. The information collected by the firm on the identity of persons described in *Commission Rule* 7.92.(c) above must at a minimum include their full name and date of birth. The extent to which the other information specified in *Commission Rule* 5.5. is obtained by the firm will depend on the likelihood of that person benefiting from the trust, with such an assessment documented. All information on the identity of that natural person specified under *Commission Rule 5.5.* must be collected and the identity of that person verified by the firm in accordance with *Commission Rule* 5.8. prior to any distribution of trust assets in accordance with *Commission Rule* 7.107., unless *Commission Rule* 7.108. applies. For the avoidance of doubt where a *legal person* or a *legal arrangement* has been identified as "any other person" the firm must apply this rule to its *beneficial owner/s*.

96. Information on the verification of the *beneficial owners* of a trust can be found in Section 7.10.3. of this *Handbook*.

7.10.2. Obligations when Dealing with Trusts or Other Legal Arrangements

97. Where a trust is a *key principal* to a *business relationship* or *occasional transaction*, the firm must:

(a) identify and verify the identity of the trust (or take reasonable measures to do so in accordance with Paragraph 4(3)(c) or (d) of *Schedule 3*), including without limitation:

(i) the full name;
(ii) the powers that regulate and bind the trust or similar *legal arrangement* and any official identification number (for example, a tax identification number or registered charity or NPO number, where relevant); and
(iii) the date and place of establishment of the trust;

(b) identify and take reasonable measures to verify the identity of the trustees of the trust, unless, in accordance with Section 9.6., they are themselves subject to this *Handbook*;
(c) require the trustees (or equivalent) of the trust or other *legal arrangement* to provide the firm with details of the identities of the *beneficial owners* of the trust, including:

(i) the *settlor(s)*, including the initial *settlor(s)* and any persons or *legal arrangements* subsequently settling *funds* into the trust;
(ii) any *protector(s)*, enforcer(s) and co-trustee(s);

(iii) any beneficiary (whether his or her interest under the trust is vested, contingent or discretionary and whether that interest is held directly by that person or as the *beneficial owner* of a *legal person* or a *legal arrangement* that is a beneficiary of the trust), any class of beneficiaries and any other person who to the best of the trustee's knowledge, is likely to benefit from the trust; and

(iv) any other natural person who exercises ultimate effective control over the trust; and

(d) understand the nature of the trust or other *legal arrangement's* business and its ownership and control structure and the purpose and intended nature of the *business relationship* or *occasional transaction*.

98. When verifying the identity of the trust in accordance with *Commission Rule* 7.97.(a), the firm does not need to obtain copies of the entire trust instrument (for example, trust deed or declaration of trust); obtaining copies of relevant extracts of such an instrument may suffice.

99. When collecting from the trustees information on the identity of persons described in *Commission Rule* 7.97.(c)(iii) above, the firm must at a minimum obtain their full name and date of birth. The extent to which the other information specified in *Commission Rule* 5.5. is obtained by the firm will depend on the likelihood of that person benefiting from the trust, with such an assessment documented. All information on the identity of that natural person specified under *Commission Rule* 5.5. must be collected and the identity of that person verified by the firm in accordance with *Commission Rule* 5.8. prior to any distribution of trust assets in accordance with *Commission Rule* 7.107., unless *Commission Rule* 7.108. applies. For the avoidance of doubt where a *legal person* or *legal arrangement* has been identified as "any other person" the firm must apply this rule to its *beneficial owner/s*.

100. Where the *business relationship* or *occasional transaction* has been assessed as high *risk*, the firm must obtain relevant extracts of the trust deed, deeds of amendments and letter(s) of wishes (as applicable to verify the points covered by *Commission Rule* 7.97.(a)(i)-(iii) above), together with an appropriate assurance from the trustee that the content of such *documents* does not contain contradictory information with other *identification data* gathered.

101. In identifying any person who is likely to benefit from the trust in accordance with *Commission Rule* 7.97.(c)(iii), the firm should seek to establish from the trustee whether there are persons, other than beneficiaries identified in the trust deed, who are likely to benefit from the trust, for example, persons named in a letter of wishes or other related *documents*.

102. Where *documents* obtained are copies of the originals, the firm should refer to the requirements of Section 6.6. of this *Handbook*.

7.10.3. Verifying the Identity of the Beneficial Owners of Trusts or Other Legal Arrangements

103. In accordance with Paragraph 4(3) of *Schedule 3*, in relation to a trust the firm shall take measures to understand the nature of the trust or *legal arrangement's* business and its ownership and control structure and identify and take reasonable measures to verify the identity of the *beneficial owner*.

104. In accordance with Paragraph 22(8) of *Schedule 3*, in relation to a trust *beneficial owner* means:

(a) any beneficiary who is a natural person, whether his or her interest under the trust is vested, contingent or discretionary, and whether that interest is held directly by that person or as the *beneficial owner* of a *legal person* or *legal arrangement* that is a beneficiary of the trust;

(b) any trustee, *settlor*, *protector* or enforcer of the trust who is a natural person or that is a *transparent legal person*;
(c) if any trustee, *settlor*, *protector* or enforcer of the trust is a *legal person* (other than a *transparent legal person*) or a *legal arrangement*, any natural person who is the *beneficial owner* of that *legal person* or *legal arrangement*;
(d) any natural person (other than a beneficiary, trustee, *settlor*, *protector* or enforcer of the trust), who has, under the trust deed of the trust or any similar document, power to:

(i) appoint or remove any of the trust's trustees;
(ii) direct the distribution of *funds* or assets of the trust;
(iii) direct investment decisions of the trust;
(iv) amend the trust deed; or
(v) revoke the trust;

(e) any *transparent legal person* (other than a trustee, *settlor*, *protector* or enforcer of the trust) that holds any of the powers set out in (d);
(f) where a *legal person* (other than an *transparent legal person*) or *legal arrangement* holds any of the powers within subparagraph (d) (other than a trustee, *settlor*, *protector* or enforcer of the trust), any natural person who is a *beneficial owner* of that *legal person* or *legal arrangement*; and
(g) any other natural person who exercises ultimate effective control over the trust.

105. In the case of a *legal arrangement* other than a trust, in accordance with Paragraph 22(9) of *Schedule 3*, *beneficial owner* means any natural person or *transparent legal person* who is in a position in relation to that *legal arrangement* that is equivalent to the position of any natural person or *transparent legal person* set out in Paragraph 22(8) of *Schedule 3* as set out above.

106. For the avoidance of doubt, the firm should treat a *transparent legal person* as a natural person for the purposes of *Schedule 3* and this *Handbook*. In doing so, the *transparent legal person* should be identified and its identity verified in accordance with *Commission Rule* 7.30. However, the firm does not need to determine the beneficial ownership of the *transparent legal person*.

107. Other than where a *business relationship* or *occasional transaction* has been assessed as being high *risk*, the firm must take reasonable measures to verify the identity of any natural person who is a beneficiary of, or any other natural person who benefits from, the trust prior to any distribution of trust assets to (or on behalf of) that natural person.

108. Where a *business relationship* or *occasional transaction* has been assessed as being high *risk*, the firm must, where possible, take reasonable measures to verify the identity of all beneficiaries and other persons who are likely to benefit from the trust at the time that the assessment of *risk* is made as set out in *Commission Rules* 7.95. and 7.99. Where it is not possible to do so (for example, because the beneficiaries have not yet been born or are excluded) the reasons must be documented and retained on the relevant *customer's* file.

109. The vast majority of trusts established and administered in *the Bailiwick* are discretionary trusts. Under a discretionary trust the beneficiaries have no right to any ascertainable part of the income or capital of the trust property. Rather, the trustees are vested with a power, which they are obliged to consider exercising, to pay the beneficiaries, or apply for their benefit, such part of the income or capital of the trust as the trustees think fit. Consequently, a beneficiary's interest in trust property is merely discretionary except to the extent that the trustee has decided to appoint a benefit to him or her.

110. *Schedule 3* recognises the differences between the interests of beneficiaries under discretionary trusts, as well as those under *fixed trusts* whose interests have not yet arisen and who are,

therefore, contingent beneficiaries. In this respect, *Commission Rule* 7.107. allows, other than in relation to *high risk relationships*, for the verification of the identity of a beneficiary to take place at the time that a distribution of trust assets or property occurs to, or on behalf of, that beneficiary.

111. Where the beneficiaries of a trust are designated by characteristics or by class, the firm must obtain sufficient information concerning the beneficiaries to *satisfy* itself that it will be able to identify, and verify the identity of, a beneficiary at the time of a distribution or when the beneficiary gains vested rights, for example, a beneficiary who is unaware of their beneficiary status until a point in time or a minor who reaches the age of majority.

112. The firm must take reasonable measures to verify the identity of those *beneficial owners* exercising control over the affairs of the trust, i.e. any *settlor(s)*, trustee(s), *protector(s)* and enforcer(s), including the *beneficial owners* of such entities where they are *legal persons* or *legal arrangements*, before or during the course of establishing a *business relationship* or before carrying out an *occasional transaction.*

113. Verification of the *beneficial owners* of a trust must be undertaken either by the firm itself or, provided that the *Commission Rules* in Chapter 10 of this *Handbook* are met, by requesting the trustee to provide the relevant information on the identity of such parties by way of a certificate or summary sheet.

114. For the purposes of Paragraph 4(3) of *Schedule 3* and *Commission Rule* 7.112., in taking measures to identify and reasonable measures to verify the identity of a *beneficial owner* of a corporate trustee, consideration should be given to the *ML*, *TF* and *PF risk* associated with the ownership of the corporate trustee, whether it is appropriately regulated and the influence and/or control a particular *beneficial owner* of the corporate trustee has over the business and affairs of that corporate trustee in respect of the assets of the applicable trust.

115. Where the trustee or its parent is subject to the same or equivalent provisions of the *Handbook* in the jurisdiction from which its business is conducted and where it is supervised for compliance with those provisions, it may be possible to rely on information in the public domain or provided by the trustee regarding the identity of its *beneficial owners* and its directors or other controlling persons by way of a summary sheet and/or structure chart, without the need to gather *identification data* on those individuals. Such an approach would be consistent with the following guidance from the FATF's guidance paper on applying a risk-based approach for TCSPs detailed below:

"Where the trustee is a listed entity (or an entity forming part of a listed group) or an entity established and regulated to carry on trust business in a jurisdiction identified by credible sources as having appropriate AML/CFT laws, regulations and other measures, the TCSP should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. A TCSP can rely on external evidence, such as information in the public domain, to satisfy itself as to the beneficial owner of the regulated trustee (e.g. the web-site of the body which regulates the trustee and of the regulated trustee itself)."

116. In making this determination, the firm should take note of reports and assessments by the FATF and/or FATF-style regional bodies, in particular of findings, recommendations and ratings of compliance with FATF Recommendation 28 or precursor recommendation which assesses the adequacy of supervision of trustees and document the conclusions of its assessment. The FATF's consolidated list of Mutual Evaluation Report ratings can be found below.

https://www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf

117. Where neither the trustee nor its parent is based in a jurisdiction with equivalent provisions of *the Handbook* in the jurisdiction from which its business is conducted and where it is supervised for compliance with those provisions, reasonable measures to verify the identity of the *beneficial owners* of the corporate trustee will be required. This will involve the collection of *identification data* on those *beneficial owners*, together with evidence of their ownership, for example, via copies of the share register of the corporate trustee or regulatory returns.

7.11. CDD Measures for Particular Categories of Legal Person and Legal Arrangement

118. This Section provides additional guidance to assist the firm in interpreting the preceding requirements of this Chapter when dealing with the following particular types of *legal person* or *legal arrangement* as a *customer* or other *key principal*:

1. Charities and Non-Profit Organisations;
2. Governments, Supranational Organisations and State-Owned Enterprises; and
3. Sovereign Wealth Funds.

7.11.1. Charities and Non-Profit Organisations

119. Charities and NPOs play a vital role in the world economy, as well as many national economies and social systems. Their efforts complement the activity of the governmental and business sectors in providing essential services, comfort and hope to those in need around the world.

120. It is recognised, however, that charities and NPOs are vulnerable to exploitation by criminals, terrorists and terrorist organisations. In this respect, a charitable or benevolent purpose can be used to disguise underlying terrorist or criminal involvement, both in the raising of capital and in the subsequent distribution of *funds*, as well as through the provision of logistical and other support to terrorist or criminal organisations and operations. This is of particular concern where the charity or NPO has connections with higher *risk* countries or territories.

121. Not all charities and NPOs are subject to scrutiny through legislation or registration requirements. Consequently, a criminal or terrorist organisation can exploit the inherent vulnerabilities in the regimes in some jurisdictions. Additionally, some charities and NPOs are predominantly cash orientated and present a mechanism to disguise and confuse the detection of the original source(s) of *funds*.

122. When carrying out a *relationship risk assessment*, the following are examples of *risk* factors specific to charities and NPOs which could be considered by the firm, both singly and cumulatively, in addition to those factors set out in Chapter 3 of this *Handbook*:

(a) the jurisdiction(s) within which *funds* are raised by the charity or NPO;
(b) the jurisdiction(s) within which *funds* are spent or distributed by the charity or NPO;
(c) the methods of *fund* raising utilised by the charity or NPO;
(d) the purpose for which the charity or NPO has been established; and
(e) the nature of the projects (or equivalent) for which the charity or NPO provides funding.

123. In considering the *risk* factors set out above, the firm may deem it appropriate to make a distinction between those charities or NPOs with a limited geographical remit and those with unlimited geographical scope, for example, medical and emergency relief charities. Where a charity or NPO has a defined area of benefit, it is only able to expend its *funds* within that defined area and can quite properly be transferring *funds* to that country or territory. It would otherwise be less clear why the charity or NPO should be transferring *funds* to a third country and this would therefore be unusual. The *FATF* does not expect charities and NPOs to automatically be treated as high risk, but rather assessed on the basis of the relevant risk factors present. Furthermore, the findings from the *NRA* indicate that the local NPO sector is low *risk*.

124. Where the *customer* is a trust, *foundation* or other *legal arrangement*, there may be a situation where a charity or NPO is identified as a "long-stop" beneficiary, for example, under a calamity/disaster clause (or equivalent). In such cases the firm would not be expected to consider the factors identified above when carrying out a *relationship risk assessment*, except where all other intended beneficiary arrangements have failed, or if the firm considers it appropriate in the circumstances.

125. With regard to the beneficial ownership of charities and NPOs, for the vast majority there will likely be no natural person who would be deemed to have control through ownership or other means in accordance with the definition of *beneficial owner* in *Schedule 3*. At most there may be a class of persons who stand to benefit from the charity's objectives and these will likely be self-evident from an understanding of the charity or NPO's nature and purpose. However, these persons are unlikely to have ultimate effective control over the affairs of the charity or NPO's.

126. Noting the above, where the charity or NPO is a *legal person*, the senior managing official for the purposes of establishing beneficial ownership will often be a senior member of the governing body or committee of the charity or NPO, or may extend to an executive where the governing body does not have day-to-day control over the charity's or NPO's affairs.

127. Many jurisdictions require the registration of at least a portion of charities or NPOs for the purpose of ensuring the transparency of that jurisdiction's NPO sector. Whilst on its own not sufficient as verification of the identity of a charity or NPO, registration may allow the firm to gather further information on a charity or NPO, including details on its nature and purpose, and may act to support any verification undertaken. Within *the Bailiwick* the Guernsey Registry maintains searchable registers of both registered charities and NPOs, excluding Sark (see Appendix B) and provides details of their name, reference number, purpose, principals and a contact address.

7.11.2. Governments, Supranational Organisations and State-Owned Enterprises

128. Where the *customer* in a *business relationship* or *occasional transaction*, or the *beneficial o*wner of the *customer*, is an overseas government or government department, a local authority, an agency established by the law of a foreign country or territory, a supranational organisation, or body owned (or majority owned) by any of the former, the firm should consider the measures set out within this Section.

129. Where the *customer*, or a *beneficial owner* or other *key principal* of the *customer*, is a *Bailiwick* public authority, the firm should refer to Section 9.4. of this *Handbook*.

130. Bodies engaged in public administration are different from state-owned bodies which conduct business. The nature and *risk* of the *business relationship* or *occasional transaction* will therefore differ. Public administration involves a different revenue/payment stream from that of most business and may be funded from government sources or other forms of public revenue. On the other hand, state-owned businesses may engage in a wide range of activities, some of which could involve higher *risk* factors. Such entities may be partly publicly funded and may derive some or all of their revenues from trading activities.

131. In assessing the *risk* of a *business relationship* or *occasional transaction* with, or involving, a government entity, the firm should pay particular attention to the *risk*s associated with the country or territory from which the government entity originates, together with the *risks* associated with the source of the government entity's funds and wealth.

132. When seeking to understand the ownership and control structure of the government entity in accordance with Paragraph 4(3)(c) of *Schedule 3*, the firm should consider the entity's

relationship with its home state authority. In the majority of cases, it is unlikely that there will be an identifiable natural person with control of the entity through ownership or other means. In such cases, the firm should look to identify the natural person who holds the position of a senior managing official of the government entity in accordance with Step 3 of Paragraph 7.36. above.

133. Given the nature of government and supranational entities, it is likely that the directors (or equivalent) will include individuals falling within the definition of a *PEP*. The firm should therefore be alive to the increased likelihood of the existence of such persons within a *business relationship* or *occasional transaction.*

134. Where the firm identifies that a *foreign PEP* or an *international organisation PEP* is acting on behalf of a government entity, but where the *PEP* does not fall within the definition of *beneficial owner* and where no property of that *PEP* is handled in the particular *business relationship* or *occasional transaction*, the firm should consider this factor as part of its *risk* assessment of the relationship, including consideration of the nature of the *PEP's* role and reason why the *PEP* holds such a role. Where the firm has determined that, but for the function held by the natural person, the *business relationship* or *occasional transaction* would be other than high *risk*, it is not required to apply *ECDD* measures.

135. One such example could be a government or state-level pension scheme investing in a *Bailiwick* CIS where members of the pension committee/board of trustees (or equivalent) are *PEPs* through their senior government positions but where they do not meet the definition of the senior managing official of the scheme. Those persons have no economic interest in the funds involved in the *business relationship* or *occasional transaction* (beyond any pension rights) and the *risk* of the relationship being used as a vehicle for the laundering of any personal funds is minimal.

7.11.3. Sovereign Wealth Funds

136. A Sovereign Wealth Fund ("SWF") is a state-owned investment fund used to invest in real and financial assets with the purpose of benefiting a country's economy. An SWF consists of a pool or pools of money derived from various sources including central *bank* reserves, commodity exports and foreign-exchange reserves.

137. There is a general concern that SWFs are capable of being used to meet political rather than purely financial objectives, by acquiring controlling interests in strategically important industries or destabilising economies. For this reason, understanding the nature and purpose of an SWF and the *business relationship* or *occasional transaction* is key.

138. Many SWFs are members of the International Forum of Sovereign Wealth Funds ("IFSWF"). Established in 2009 by a group of 23 state-owned international investors, the IFSWF is a global network of SWFs. The purpose of the IFSWF is to exchange views on issues of common interest with the aim of facilitating an understanding of the activities of SWFs and of the Santiago Principles which provide a clearer understanding of SWFs by promoting transparency, good governance, accountability and prudent investment practices.

139. Whilst membership alone is not sufficient as verification of an SWF, further information on the IFSWF members, including details on their ownership, nature, objects and purpose can be found on the IFSWF website and may act to support any verification undertaken.

140. When seeking to identify the *beneficial owner* of an SWF which is a *legal person*, it is unlikely that there will be an identifiable natural person with control of the SWF through ownership or by other means. In such cases the firm should look to identify the natural person who holds the position of senior managing official of the SWF in accordance with Step 3 of Paragraph 7.36. above.

7.12. CDD Measures for Particular Products and Services

141. In addition to the *CDD* measures detailed previously for *legal persons* and *legal arrangements* with which the firm deals as part of its *business relationships* and *occasional transactions*, there may be instances where the firm offers particular products or services which have unique *risks* associated with them.

142. This section provides *Commission Rules* and guidance in respect of the *CDD* measures to be applied by the firm where it provides the following products or services:

1. Life and Other Investment Linked Insurance;
2. Employee Benefit Schemes, Share Option Plans or Pension Schemes; or
3. Custody or Management to Non-Guernsey Collective Investment Schemes.

7.12.1. Life and Other Investment Linked Insurance

143. Where the product or service provided by the firm is the issuing of a life or other investment linked insurance policy, the firm must, in addition to identifying and verifying the *customer* and taking reasonable measures to verify the identity of the *beneficial owner*, also undertake the following measures in relation to any beneficiary as soon as they are identified or designated:

(a) for a beneficiary that is identified as a specifically named natural or *legal person* or *legal arrangement*, take the name of the natural or *legal person* or *legal arrangement*; and
(b) for a beneficiary that is designated by characteristics or by class (for example, a spouse or child) or by other means (for example, under a will), obtain sufficient information concerning the beneficiary for the firm to *satisfy* itself that it will be able to establish the identity of the beneficiary at the time of distribution.

144. In addition to considering whether the *beneficial owner* of a life or other investment linked insurance policy is a *PEP* in accordance with Paragraph 4(3)(f) of *Schedule 3*, the firm must also make a determination as to whether any beneficiary of such a policy (or the *beneficial owner* of a beneficiary where that beneficiary is a *legal person* or *legal arrangement*) is a *PEP* at the time that the beneficiary is identified or designated.

145. Where the firm determines that the *beneficial owner*, any beneficiary, or the *beneficial owner* of any beneficiary of a life or other investment linked insurance product is a *PEP*, the firm must act in accordance with the requirements of Paragraph 5 of *Schedule 3* and Section 8.5. of this *Handbook*.

146. Verification of the identity of any beneficiary identified in accordance with *Commission Rule* 7.143. must occur prior to any distribution to (or on behalf of) that beneficiary.

147. When carrying out a *relationship risk assessment* as required by Paragraph 3 of *Schedule 3* and Chapter 3 of this *Handbook*, the firm must include any beneficiary identified by *Commission Rule* 7.143. above as a relevant *risk* factor in considering the overall *risk* of the *business relationship* or *occasional transaction*.

148. Where the firm has determined that a beneficiary which is a *legal person* or *legal arrangement* poses a high *risk*, the firm must carry out *ECDD* measures in accordance with Chapter 8 of this *Handbook*. This must include identifying and taking reasonable measures to verify the identity of the *beneficial owner* of the beneficiary prior to any distribution to (or on behalf of) the beneficiary and to consider reporting suspicious transactions or activity.

7.12.2. Employee Benefit Schemes, Share Option Plans and Pension Schemes

149. Where the product or service provided by the firm is:

(a) an employee benefit scheme or arrangement;
(b) an employee share option plan;
(c) a pension scheme or arrangement;
(d) a superannuation scheme; or
(e) a similar scheme or arrangement;

and where contributions are made by an employer or by way of deductions from wages and the scheme rules do not permit assignment of a member's interest under the scheme, then the sponsoring employer, the trustee, the *foundation* council and any other person who has control over the *business relationship* or *occasional transaction* (for example, the administrator or the scheme manager) are to be considered as *key principals* and must be identified and verified by the firm in accordance with the requirements of *Schedule 3* and this *Handbook*.

150. Where contributions to the scheme are made by the sponsoring employer, or by way of deductions from wages or otherwise through the payroll process, there is no requirement to apply *CDD* measures to the member throughout the life of the *business relationship*. However, the firm should be alive to the *risk* associated with the disbursement of pension *funds*, for example, the receipt of fraudulent requests for payment or the member being subject to UN, UK or other sanction.

151. Where a member or other third party makes contributions to a scheme or arrangement (outside of the sponsoring employer's payroll process) which would fall within the definition of an *occasional transaction* (for example, a voluntary contribution of more than £10,000 into the scheme) or a *business relationship* (for example, following the cessation of employment, making arrangements for smaller, regular ongoing contributions), the firm must apply *CDD* measures, including *ECDD* measures and/or *enhanced measures* as appropriate, to that member or third party.

152. Where a member's interest in a scheme or arrangement is distributed to a third party (for example, a named beneficiary upon the death of the member), the firm should establish the rationale for the distribution and consider the extent of the *CDD* measures to be applied to the third party in order for the firm to satisfy itself that the third party's interest is legitimate and that the third party (for example, the beneficiary) does not pose a *risk* to the firm.

153. When carrying out a *relationship risk assessment* in accordance with Paragraph 3 of *Schedule 3* and Chapter 3 of this *Handbook*, the firm must include the natural or *legal person(s)* or *legal arrangement(s)* providing *funds* to the scheme or arrangement as a relevant *risk* factor when determining the overall *risk* of the *business relationship* or *occasional transaction*.

7.12.3. Non-Guernsey Collective Investment Schemes

154. Where the firm is providing management or custody services, within the scope of a licence issued to it by *the Commission* under *the POI Law*, to a CIS established outside *the Bailiwick* it may, in certain circumstances, place reliance on the administrator or *transfer agent* of the NGCIS to have applied *CDD* measures to the investors in that scheme.

155. Where the firm provides management or custody services and wishes to rely on the *CDD* measures of the administrator of the NGCIS, the firm must:

(a) apply *CDD* measures to the administrator or *transfer agent* to ensure that it is an *Appendix C business* and regulated and supervised for investment business; and
(b) require the administrator or *transfer agent* to provide a written confirmation which:

(i) confirms that the administrator or *transfer agent* has appropriate *risk*-grading procedures in place to differentiate between the *CDD* measures for *high risk relationships* and *low risk relationships*;
(ii) contains adequate assurance that the administrator or *transfer agent* applies the necessary *CDD* measures to the investors in the NGCIS (including the *beneficial owners* of such); and
(iii) contains an assurance that the administrator or *transfer agent* will notify the firm where an investor in the NGCIS, or the *beneficial owner* of such, is categorised as a *PEP*.

156. In addition, the firm must have a programme for reviewing the *CDD* procedures of the administrator or *transfer agent* and testing the application of those procedures in respect of the underlying investors within the NGCIS.

157. Where the firm is acting as the administrator of an NGCIS and its functions include that of registrar/*transfer agent* or similar, the firm must apply *CDD* measures to the investors into the NGCIS as if they were its *customers* in accordance with the requirements of Section 4.8.2. of this *Handbook*.

158. Where the firm is entering into a *business relationship* or conducting an *occasional transaction* with an NGCIS which is its *customer* (for example, an accountant providing services to the NGCIS) the firm should treat the NGCIS as a *legal person* or *legal arrangement* and apply *CDD* measures in accordance with the relevant sections of this Chapter.

7.13. Additional Requirements on Trustees and Partners

159. The additional requirements in this Section apply to trustees when acting as trustee of a relevant trust and to partners (excluding limited partners of limited partnerships) of relevant partnerships and limited partnerships without legal personality, which are subject to Guernsey law. They also apply to foreign trustees and partners when acting in relation to a relevant trust or relevant partnership and Guernsey trustees and partners when acting in relation to an equivalent foreign *legal arrangement*. They do not apply where the partner is acting for a limited partnership with legal personality.

7.13.1. Regulated Agents and Service Providers

160. In accordance with Paragraph 15I(1) of *Schedule 3*, a *specified business* which acts as a trustee of a relevant trust or a partner of a relevant partnership (or occupies an equivalent role to that of trustee or partner in relation to a foreign *legal arrangement*) shall hold information on the identity of any regulated agents and service providers to the relevant trust or relevant partnership.

161. In accordance with Section 51(1) of *the Law*, a relevant partnership means;
(a) a limited partnership within the meaning of, and subject to the provisions of, the Limited Partnerships (Guernsey) Law, 1995 that does not have legal personality, or
(b) a partnership within the meaning of, and subject to the provisions of, the Partnership (Guernsey) Law, 1995.

162. In accordance with Section 51(1) of *the Law*, a relevant trust means any *express trust* that is governed by or is otherwise subject to the law of any part of *the Bailiwick*.

163. In accordance with Paragraph 21 of *Schedule 3*, a regulated agent means a person who;
   a) is acting in relation to or on behalf of a relevant trust or relevant partnership, as the case may be, and
   b) for the purposes of so doing is required to hold, and does hold, a licence from *the Commission* or a corresponding body in another jurisdiction.

164. In accordance with Paragraph 21 of *Schedule 3*, the term service provider referred to within Paragraph 15I(1) of *Schedule 3* means a person, who is providing investment advisory or management services, managerial services, accountancy services, tax advisory services, legal services, trust services, partnership services or corporate services in relation to a relevant trust or relevant partnership, as the case may be. It does not apply in respect of the provision of these services to an underlying company of a relevant trust or relevant partnership.

165. The information held on the identity of persons described in Paragraph 15I(1) of *Schedule 3* by the *specified business* which acts as a trustee of a relevant trust or partner of a relevant partnership (or occupies an equivalent role to that of trustee or partner in relation to a foreign *legal arrangement*) must include:

Where it is a legal person or legal arrangement;
(a) the name of the legal person or legal arrangement, including any trading names;
(b) registered office address; and
(c) any official identification number.

Where it is an individual;
(a) legal name; and
(b) principal residential address.

166. In accordance with Paragraph 15I(2) of *Schedule 3*, a *specified business* shall ensure that the information it holds on the identity of any regulated agents and service providers to the relevant trust or relevant partnership:

(a) so far as is possible, is accurate and up to date; and
(b) is updated on a timely basis.

167. In order to ensure that the information is accurate the firm should consider how the information has been obtained and whether to undertake searches on publicly available sources from any registry, regulatory authority or supervisory body if it has doubts about the information.

168. Sufficient information is likely to be held on their identity through correspondence with the regulated agent or service provider and the reports the firm receives. The Commission will not specify how the information is held, but would expect the firm to be able to access the information in a timely manner should it be asked for by the relevant authorities.

169. The information obtained within this section is considered to be *CDD information* and must be retained in accordance with the record keeping requirements in both Paragraph 14(2) of *Schedule 3* and Chapter 16 of this *Handbook*.

7.13.2. Disclosures for Trustees and Partners

170. In accordance with Paragraph 15J(1) of *Schedule 3*, where a *specified business* enters into a *business relationship* or carries out or is otherwise involved in an *occasional transaction* with a *financial services business* or a relevant business, and it is acting in its capacity as a trustee of a relevant trust or partner of a relevant partnership (or the occupant of an equivalent role in relation

to a foreign *legal arrangement*), it shall disclose the capacity in which it is so acting to the *financial services business* or relevant business in question.

171. Where a *specified business* is acting on behalf of a relevant trust or relevant partnership (or occupies an equivalent role to that of trustee or partner in relation to a foreign *legal arrangement*), the *specified business* could meet the above disclosure requirement by referencing its capacity in its sign off, for example, "as trustee of the [trust name] trust" or "as (general) partner of the [partnership name] partnership". Other forms of disclosures will also be acceptable, providing it is documented and clear that it has been disclosed to the *financial service business* or relevant business in question.

172. In accordance with Paragraph 15K(1) of *Schedule 3*, a *specified business* which acts as a trustee of a relevant trust or partner of a relevant partnership (or occupies an equivalent role to that of trustee or partner in relation to a foreign *legal arrangement*) may disclose upon request to any relevant authorities information relating to the trust or partnership, and to a *financial services business* or a relevant business, any information relating to the beneficial ownership of the trust or partnership and any assets of the trust or partnership that are to be held or managed under the terms of a business relationship or occasional transaction.

173. Paragraph 15K(1) of *Schedule 3* ensures that a *specified business* acting as a trustee of a relevant trust or partner of a relevant partnership (or occupies an equivalent role to that of trustee or partner in relation to a foreign *legal arrangement*) is legally permitted to disclose information about the trust or partnership's beneficial ownership and assets to the relevant authorities, and to other financial institutions or obliged entities with whom the *specified business*, in its capacity as trustee or partner, is entering into a business relationship or occasional transaction, to enable them to fulfil their due diligence obligations. It does not provide authority to a *specified business* to breach *the Data Protection Law*.

Chapter 8
Enhanced Customer Due Diligence

Contents of this Chapter

8.1. Objectives

1. This Chapter relates to *business relationships* and *occasional transactions* which have been assessed by the firm as:

   (a) presenting a high *risk* of *ML*, *TF* and/or *PF* taking into account the requirements of Paragraph 5(1) of *Schedule 3*; and/or
   (b) involving one or more of the higher *risk* factors set out in Paragraphs 5(2)(a)-(d) of *Schedule 3*

   and should be read in conjunction with Chapter 3 of this *Handbook* which provides *Commission Rules* and *guidance* on the assessment of *risk* and Chapters 4 to 7 of this *Handbook* which set out the *CDD* measures to be applied.

2. In accordance with Paragraph 5(1) of *Schedule 3*, where the firm is required to carry out *CDD*, it shall also carry out *ECDD* in relation to high *risk business relationships* and *occasional transactions*, including, without limitation -

   (a) a *business relationship* or *occasional transaction* in which the *customer* or any *beneficial owner* is a *foreign PEP* (see Section 8.5. of this *Handbook*),
   (b) where the firm is an *FSB*, a *business relationship* which is -

      (i) a *correspondent banking relationship*, or
      (ii) similar to such a relationship in that it involves the provision of services, which themselves amount to financial services business or facilitate the carrying on of such business, by one *FSB* to another (see Section 8.6. of this *Handbook*),

   (c) a *business relationship* or *occasional transaction* -

      (i) where the *customer* or *beneficial owner* has a *relevant connection* with a country or territory that -

         (A) provides funding or support for terrorist activities, or does not apply (or insufficiently applies) *the FATF Recommendations*, or
         (B) is a country otherwise identified by the FATF as a country for which such measures are appropriate (see Section 8.7. of this *Handbook*),

      (ii) which the firm considers to be a *high risk relationship*, taking into account any notices, instructions or warnings issued from time to time by *the Commission* and having regard to the *NRA*,

   (d) a *business relationship* or an *occasional transaction* which has been assessed as a *high risk relationship*, and
   (e) a *business relationship* or an *occasional transaction* in which the *customer*, the *beneficial owner* of the *customer*, or any other *legal person* in the ownership or control structure of the *customer*, is a *legal person* that has *bearer shares* or *bearer warrants* (see Section 8.8. of this *Handbook*).

3. In accordance with Paragraph 5(2) of *Schedule 3*, the firm shall also carry out *enhanced measures* in relation to *business relationships* and *occasional transactions*, whether otherwise high *risk* or not, which involve or are in relation to -

   (a) a *customer* who is not resident in *the Bailiwick* (see Section 8.9. of this *Handbook*);
   (b) the provision of private banking services (see Section 8.10. of this *Handbook*);

(c) a *customer* which is a *legal person* or *legal arrangement* used for personal asset holding purposes (see Section 8.11. of this *Handbook*); or

(d) a *customer* which is –

(i) a *legal person* with *nominee shareholders*, or

(ii) owned by a *legal person* with *nominee shareholders* (see Section 8.12. of this *Handbook*).

4. Paragraphs 5(1) and 5(2) of *Schedule 3* are distinct from one another. Paragraph 5(1) requires that *ECDD* measures are applied to all *high risk relationships*. The requirement to apply *enhanced measures* to mitigate particular higher *risk* factors as set out in Paragraph 5(2) of *Schedule 3* can apply to *business relationships* and *occasional transactions* across the *risk* spectrum from low to high *risk*.

5. The presence of one or more of the higher *risk* factors set out in Paragraph 5(2) of *Schedule 3* may not necessarily equate to the overall *risk* of the *business relationship* or *occasional transaction* being high. However, in accordance with *Commission Rule* 3.19., the firm must have regard to the cumulative effect that one or more of these factors could have on the overall *risk* of the *business relationship* or *occasional transaction* when conducting a *relationship risk assessment*.

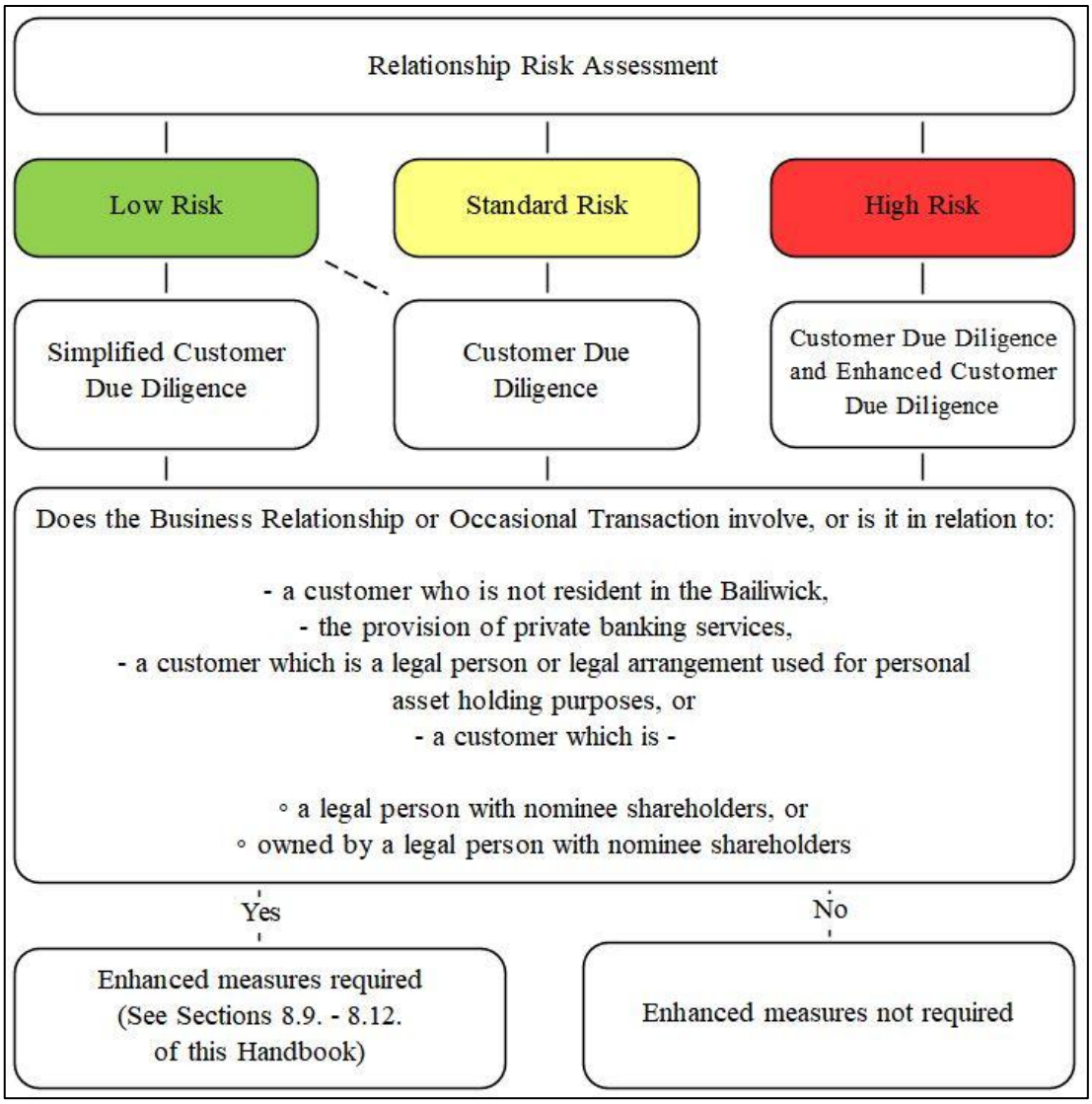


Fig. 10 – Enhanced Measures Flowchart

Nature of *Business Relationship* or *Occasional Transaction*	Measures to be Applied
Low risk relationship exhibiting one or more of the higher *risk* factors set out in Paragraph 5(2) of *Schedule 3*.	*SCDD* or *CDD* measures, together with *enhanced measures* appropriate to the higher *risk* factor(s) present.
Standard *risk business relationship* or *occasional transaction* exhibiting one or more of the higher *risk* factors set out in Paragraph 5(2) of *Schedule 3*.	*CDD* measures, together with *enhanced measures* appropriate to the higher *risk* factor(s) present
High risk relationship which meets one or more of the criteria in Paragraph 5(1) of *Schedule 3*.	*CDD* measures, together with *ECDD* measures as set out in Section 8.2.1. of this *Handbook*
High risk relationship which meets one or more of the criteria in Paragraph 5(1) of *Schedule 3* and exhibits one or more of the higher *risk* factors set out in Paragraph 5(2) of *Schedule 3*.	*CDD* measures and *ECDD* measures as set out in Section 8.2.1. of this *Handbook*, together with *enhanced measures* appropriate to the higher *risk* factor(s) present.

Fig. 11 – Application of Due Diligence and Enhanced Measures Depending on Risk

8.2. Policies, Procedures and Controls

8.2.1. ECDD Measures (High Risk Relationships)

6. The firm must ensure that its policies, procedures and controls require the application of *ECDD* measures where the firm has determined, taking into account the circumstances set out in Paragraph 5(1) of *Schedule 3* and the *risk* factors provided in Chapter 3 of this *Handbook*, that a *business relationship* or *occasional transaction* is high *risk*.

7. In accordance with Paragraph 5(3)(a) of *Schedule 3*, references to *ECDD* shall mean -

(i) obtaining senior management approval for establishing a *business relationship* or undertaking an *occasional transaction*,

(ii) obtaining senior management approval for, in the case of either –

(A) an existing *business relationship* with a *foreign PEP*, or

(B) an existing high *risk business relationship* with a *domestic or international organisation PEP*,

continuing that *business relationship*,

(iii) taking reasonable measures to establish and understand the source of any *funds* and of the wealth of –

(A) the *customer*, and

(B) the *beneficial owner*, where the *beneficial owner* is a *PEP*,

(iv) carrying out more frequent and more extensive ongoing monitoring, including increasing the number and timing of controls applied and selecting patterns of activity or transactions that need further examination in accordance with Paragraph 11 of *Schedule 3* (see Chapter 11 of this *Handbook*), and

(v) taking one or more of the following steps as would be appropriate to the particular *business relationship* or *occasional transaction*,

(A) obtaining additional information about the *customer*, such as the type, volume and value of the *customer's* assets and additional information about the *customer's beneficial owners*,

(B) verifying additional aspects of the *customer's* identity,

(C) obtaining additional information to understand the purpose and intended nature of each *business relationship* and *occasional transaction*, and
(D) taking reasonable measures to establish and understand the source of wealth of *beneficial owners* not falling within Paragraph 5(3)(iii).

8. Examples of steps the firm could take in accordance with Paragraphs 5(3)(v)(A)-(D) of Schedule 3 could include:

(a) supplementing the firm's understanding of the purpose and intended nature of the *business relationship* by obtaining information on the reasons for intended or performed transactions;
(b) commissioning independent research by a specialist firm or consultant, pertaining to the purpose and objective of the *business relationship* or *occasional transaction* and evidencing information in relation to the *customer* and/or the *beneficial owner*;
(c) where the *customer* is a *legal person*, identifying, and verifying the identity of, other directors (or equivalent) of the *customer* in addition to those senior managing officials identified as *beneficial owners* in accordance with Step 3 of Paragraph 7.36. of this *Handbook* and/or those natural persons acting on behalf of the *customer* captured by Section 4.3.2.;
(d) obtaining internal information from group representatives or offices based in a jurisdiction where the *customer* has a connection; and/or
(e) using AI to identify credible independent references about the *customer* or *beneficial owner* for the firm's due diligence considerations to draw on.

9. In addition to the requirements of Paragraph 5(3) of *Schedule 3* as set out above, listed below are examples of further steps the firm could take as part of its *ECDD* measures to address specific *risks* arising from a *high risk relationship*:

(a) in the case of an existing *business relationship* which has, following a *relationship risk assessment*, been assessed as high *risk* not involving a *foreign PEP*, obtaining senior management approval for continuing that relationship; and/or
(b) requiring the first payment be carried out through an *account* in the *customer's* name with an *Appendix C business*.

8.2.2. Enhanced Measures (Higher Risk Factors)

10. In accordance with Paragraph 5(2) of *Schedule 3*, the firm's policies, procedures and controls must require the application of *enhanced measures* as detailed in Sections 8.9. - 8.12. of this *Handbook* to *business relationships* and *occasional transactions* involving or in relation to one or more of the higher *risk* factors in Paragraph 5(2)(a)-(d) of *Schedule 3*.

11. There may be a *business relationship* or *occasional transaction* which involves or is in relation to more than one of the higher *risk* factors set out in Paragraph 5(2)(a)-(d) of *Schedule 3* (for example, a non-resident *customer* using private banking services). In such cases, the firm must apply *enhanced measures* sufficient to mitigate each of the higher *risk* factors present within the *business relationship* or *occasional transaction*.

8.2.3. ECDD and Enhanced Measures (High Risk Relationships with Higher Risk Factors)

12. There may also be circumstances in which a *high risk relationship* involves or is in relation to one or more of the higher *risk* factors in Paragraph 5(2)(a)-(d) of *Schedule 3*. In such cases the firm must apply *ECDD* measures as well as applying sufficient *enhanced measures* to mitigate the particular higher *risk* factor(s) present.

13. In accordance with *Commission Rule* 8.12. above, the *enhanced measures* applied by the firm should be specific to the particular higher *risk* factor(s) present in a *business relationship* or *occasional transaction*. However, there may be situations where an *enhanced measure* taken by the firm addresses more than one higher *risk* factor, or where the *ECDD* measures applied by the firm to a *high risk relationship* also mitigate one or more higher *risk* factor(s).

14. For example, it may be that the firm is providing private banking services to a *customer* who is a *foreign PEP* and the firm is *satisfied* that the *ECDD* measures applied to address the fact that the *customer* is a *PEP* equally mitigate the higher *risk* associated with the provision of private banking services (for example, by taking reasonable measures to establish the source of *funds* and the source of the *customer's* wealth).

15. The policies, procedures and controls of the firm should allow for it to determine, based upon the specific higher *risk* factors present in a *business relationship* or *occasional transaction* and its assessment of the overall *risk* of that relationship, which and how many *enhanced measures* it would be appropriate to apply to mitigate the specific *risks* identified.

8.3. Source of Funds and Source of Wealth

16. In accordance with Paragraph 5(3)(a)(iii) of *Schedule 3*, as part of its *ECDD* measures the firm shall take reasonable measures to establish and understand the source of any *funds* and of the wealth of –

    (A) the *customer*, and
    (B) the *beneficial owner*, where the *beneficial owner* is a *PEP*.

17. The taking of reasonable measures to establish and understand a *customer's* source of wealth (and that of any *beneficial owner* who is a *PEP*), together with measures to establish and understand the source of any *funds* used in a *business relationship* or *occasional transaction*, are important aspects of the due diligence process. These steps serve to assist the firm in *satisfying* itself that such wealth and *funds* are not the *proceeds* of criminal activity and are consistent with the firm's knowledge of the *customer* and *beneficial owner*, and the nature of the *business relationship* or *occasional transaction.*

18. In addition to taking reasonable measures to establish the source of any *funds* and of the wealth of the *customer*/*beneficial owner* for *high risk relationships* as part of *ECDD* measures, the firm may also determine that it would be appropriate to apply the measures in Paragraph 5(3)(a)(iii) of *Schedule 3* as an *enhanced measure* to apply to a *business relationship* or *occasional transaction* involving or in relation to one or more of the higher *risk* factors in Paragraph 5(2) of *Schedule 3* but where the overall *risk* of the *business relationship* or *occasional transaction* is other than high.

19. The source of *funds* refers to the activity which generated the particular *funds* for a *business relationship* or *occasional transaction*. Source of wealth is distinct from source of *funds* and describes the activities which have generated the total net worth of the *customer* or *beneficial owner* both within and outside a *business relationship*, i.e. those activities which have generated a *customer's* or *beneficial owner's* net assets and property.

20. The firm must, in taking reasonable measures to establish the source of any *funds* and wealth, document and evidence consideration of the *risk* implications of the source of the *funds* and wealth and the geographical sphere of the activities in which they have been generated.

21. In determining what constitutes 'reasonable measures' to establish the source of *funds* and wealth, i.e. show them to be true, the firm should have regard to the particular *risk* factors present

in a *business relationship* or *occasional transaction*, together with its overall assessed *risk*. Such *risk* factors include, inter alia, the value of the *customer's* or *beneficial owner's* assets, together with the value of the *funds* involved in the *business relationship* or *occasional transaction*, the type and complexity of the *customer* or *beneficial owner*, the *customer's* or *beneficial owner's* economic activity and employment, and the nature of the services provided by the firm.

22. Information on the source of *funds* and wealth will generally be obtained from the *customer* or *beneficial owner* in the first instance and the extent to which this is corroborated through additional information or documentation should be commensurate with the *risk*. The firm may have a *business relationship* where it can establish to its satisfaction the source of *funds* and source of wealth from the *customer* or *beneficial owner* without seeking to corroborate that information because it is consistent with the knowledge the firm holds about the *business relationship* or *occasional transaction* and because the values involved are relatively low and commensurate with the type of product or service being provided by the firm.

23. For example, the firm may have a natural person *customer* located in a higher *risk* jurisdiction utilising its products or services for a relatively small amount of *funds* and where the firm has determined that the only factor making it a *high risk relationship* is geographic *risk*. In such a case placing reliance upon the information provided by the *customer* on the source of *funds* and wealth as part of the firm's *ECDD* measures could be considered 'reasonable' because it is consistent with the information and knowledge it has built up about the *customer* through *CDD* measures, together with the other elements of its *ECDD* measures and the *enhanced measures* applied because the *customer* is not resident in *the Bailiwick*.

24. On the other hand, 'reasonable measures' will require corroborating information where the *customer* or *beneficial owner* is from a higher *risk* country or territory, where the values involved in the *business relationship* or *occasional transaction* are large and where the sources of *funds* and wealth are not easily discernible from the *customer's* or *beneficial owner's* disclosed income and business interests.

25. The extent to which the firm corroborates the information provided by the *customer* or *beneficial owner* on the source of *funds* and wealth is a function of *risk* and not a 'one size fits all' approach. Where corroboration of the information provided by the *customer* or *beneficial owner* is required, the firm could consider one or more of the means set out in the following non-exhaustive list:

    (a) commissioning an independent and reliable report from a specialist agency;
    (b) obtaining certified copies of corroborating documentation such as contracts of sale, property deeds, salary slips, etc.;
    (c) where the firm is part of a group, obtaining reliable information from another member of the group with which the *customer* or *beneficial owner* has a connection
    (d) where the source of funds or source of wealth include virtual assets, using blockchain analysis products, or other suitable services, from a reliable commercial vendor;
    (e) obtaining information from a reliable third party (for example, a professionally qualified solicitor, accountant or tax advisor) who has an office in a country or territory connected with the *customer* or *beneficial owner*;
    (f) where the *customer* has been introduced to the firm, obtaining information from the *introducer*;
    (g) where information is publicly available, whether identified through online searches, through searches by AI, or available through subscription services, obtaining information from a reliable public or private third party source; or
    (h) obtaining information from financial statements that have been prepared and audited in accordance with generally accepted accounting principles.

26. It would not be considered sufficient for the firm to accept a *customer's* or *beneficial owner's* responses on an application form at face value, particularly where vague answers are given (for

example, ‘employment’ or ‘salary’) without further clarification. As noted previously, the firm should seek to corroborate the source of *funds* and source of wealth, particularly where the value of *funds*, or the *risk* of the *business relationship* or *occasional transaction*, is high, for example, by taking steps to understand where the *customer* or *beneficial owner* was employed and his or her actual level of income.

27. Similarly, establishing the source of *funds* involved in a *business relationship* or *occasional transaction* should not be limited to knowing from which financial institution the *funds* may have been transferred. The steps taken by the firm should be substantive and seek to establish the provenance of the *funds* or the reason for the *funds* having been acquired.

28. The obligation to take reasonable measures to establish the source of *funds* extends beyond those *funds* present at the commencement of a *business relationship*. In this respect, the firm’s monitoring arrangements should include assessing, on an ongoing basis, whether the transactional activity of a *business relationship* is consistent with the *risk* profile of that relationship, the nature of the product provided and the firm’s understanding of the *customer’s* and *beneficial owner’s* source of wealth.

8.4. Interplay Between SCDD and Enhanced Measures

29. It may be possible to apply *SCDD* measures as specified in Chapter 9 of this *Handbook* to a *business relationship* or *occasional transaction* involving or in relation to one or more of the higher *risk* factors set out in Paragraph 5(2) of *Schedule 3*, provided that *enhanced measures* are applied to address the particular higher *risk* factors present.

30. By way of example, it may be possible, where the firm has assessed the *ML, TF* and *PF risk* of a *business relationship* or *occasional transaction* to be low, to apply the *SCDD* measures set out in Section 9.3. of this *Handbook* to a natural person resident in *the Bailiwick* using a personal asset holding vehicle, provided the firm also applies an *enhanced measure* to satisfy itself that the use of such a personal asset holding vehicle is genuine and legitimate.

31. Similarly it may be possible, where the firm has assessed the *ML, TF* and *PF risk* as low, to apply the *SCDD* measures set out in Section 9.6. of this *Handbook* to a non-resident *Appendix C business*, provided that an *enhanced measure* is also applied to mitigate the *risk* associated with a non-resident *customer*, for example, to determine and understand why the *Appendix C business* is obtaining the services in *the Bailiwick* and not in its home jurisdiction.

ECDD Measures

8.5. Politically Exposed Persons

8.5.1. Introduction

32. Due to their position and influence, *PEPs* may have the potential to abuse their positions for the purpose of committing *ML* and related predicate offences, including bribery and corruption, as well as conducting activity related to *TF* and *PF*. Where a *PEP* also has connections to countries or business sectors where corruption is widespread, the *risk* is further increased.

33. *PEP* status itself does not incriminate individuals or their associates and connected entities. However, it will mean that a *customer* or *beneficial owner* who is a *foreign PEP* is subject to *ECDD* measures and that a *domestic PEP* or *international organisation PEP* may, on the basis of *risk*, be subject to *ECDD* measures.

34. There is no 'one-size fits all' approach to applying *ECDD* measures for *PEPs*. The nature of the measures applied will be commensurate with the type of *PEP*, the specific *risks* that are identified and the nature of the *PEP's* position and ability to influence.

8.5.2. Identification of PEPs

35. In accordance with Paragraph 4(3)(f) of *Schedule 3*, as part of its *CDD* measures the firm shall make a determination as to whether the *customer* or *beneficial owner* is a *PEP*, and if so, whether he or she is a *foreign PEP*, a *domestic PEP* or an i*nternational organisation PEP*.

36. As referenced above, Paragraph 5(4) of *Schedule 3* defines three categories of *PEP*, referred to as follows for the purpose of this *Handbook*:

(a) "*foreign PEP*" – a natural person who has, or has had at any time, a prominent public function, or who has been elected or appointed to such a function, in a country or territory other than *the Bailiwick*;
(b) "*domestic PEP*" – a natural person who has, or has had at any time, a prominent public function, or who has been elected or appointed to such a function, within *the Bailiwick*; and
(c) "*international organisation PEP*" – a natural person who is, or has been at any time, entrusted with a prominent function by an *international organisation*.

37. In accordance with the definition of *PEP* contained within Paragraph 5(4) of *Schedule 3*, prominent public function includes, without limitation -

(i) heads of state or heads of government;
(ii) senior politicians and other important officials of political parties;
(iii) senior government officials;
(iv) senior members of the judiciary;
(v) senior military officers; and
(vi) senior executives of state owned body corporates.

38. When seeking to establish whether a natural person falls within the definition of a *PEP*, 'prominent' should be interpreted as relating only to those persons in positions of seniority in the areas covered by Paragraph 8.37. above. Middle ranking or more junior individuals in the foregoing categories are explicitly excluded from the definition.

39. Notwithstanding the above, the term 'prominent' is not defined either in *Schedule 3* or this *Handbook* as the precise level of seniority which triggers the requirement to treat an individual as a *PEP* will depend upon a range of factors, including the role held by the individual, the particular organisational framework of the government or *international organisation* concerned, and the powers, responsibilities and influence associated with particular public functions.

40. In accordance with Paragraph 5(5A) of *Schedule 3*, a person is not a *PEP* for the purposes of *Schedule 3* if that person –

(a) was not a *PEP* within the meaning of Regulation 5(2)(b) of *the FSB Regulations* or Regulation 5(2)(b) of *the PB Regulations*, when those regulations were in force, and
(b) ceased to be entrusted with a prominent public function in respect of *the Bailiwick* before 31 March 2019.

41. To assist in the identification of natural persons falling within the definition of *domestic PEP*, Appendix E to this *Handbook* lists those positions in Guernsey, Alderney and Sark deemed to fall within the categories listed in Paragraph 8.37. above. Where an individual ceased to hold a

prominent public function listed in Appendix E prior to 31 March 2019, in accordance with Paragraph 5(5A) of *Schedule 3* there is no requirement for the individual to be identified as a *PEP*, or to consider as part of its *relationship risk assessment* the implication of the person having held a prominent public function in *the Bailiwick*.

42. Authorities in other jurisdictions may publish lists, similar to Appendix E to this *Handbook*, of those natural persons considered to fall within the definition of a *PEP* within their jurisdiction. These could be helpful for the firm in determining whether to treat an individual as a *PEP*. However, the firm should be mindful that these classifications will be based upon perceptions of *risk* applicable within other jurisdictions and that these may not necessarily be appropriate perceptions from the perspective of the firm.

43. In determining whether a *customer* or *beneficial owner* is a *PEP*, the firm could consider:

(a) using sources such as the UN, the EU, the UK Foreign and Commonwealth Office and the Group of States Against Corruption to establish, as far as is reasonably possible, whether or not a *customer* or *beneficial owner*, is a natural person who is the current or former holder of a prominent public function in a foreign country or territory, or for an *international organisation*;
(b) using sources such as the States of Guernsey, States of Alderney and Chief Pleas of Sark to establish, as far as is reasonably possible, whether or not a *customer* or *beneficial owner* is a natural person who is the current or former holder of a prominent public function within *the Bailiwick*;
(c) seeking confirmation from a *customer* or *beneficial owner*, for example through a question within an application form, as to whether they hold, or have held, a prominent public function either within *the Bailiwick* or beyond, or for an *international organisation*; or
(d) using commercially available databases to identify such persons.

44. In accordance with Paragraph 5(1)(a) of *Schedule 3, w*here the firm determines that an individual who is the *customer* or *beneficial owner* to a *business relationship* or *occasional transaction* is a *foreign PEP*, it shall carry out *ECDD* in relation to that *business relationship* or *occasional transaction*.

45. Where the firm identifies that a *customer* or *beneficial owner* is a *domestic PEP* or *international organisation PEP*, it must gather sufficient information to understand the particular characteristics of the public function that the natural person has been entrusted with and factor this information into the *relationship risk assessment* conducted in accordance with Paragraph 3 of *Schedule 3* and Chapter 3 of this *Handbook*.

46. Where, having conducted a *relationship risk assessment*, the firm concludes that the *business relationship* or *occasional transaction* involving a *domestic PEP* or *international organisation PEP* is high *risk*, the firm must apply *ECDD* measures in accordance with Paragraph 5(3)(a) of *Schedule 3* and Section 8.2.1. of this *Handbook*.

47. Where the firm concludes that the *business relationship* or *occasional transaction* with the *domestic PEP* or *international organisation PEP* does not present a high level of *risk*, it is not necessary to apply *ECDD* measures, provided that the firm has applied *SCDD* or *CDD* measures and any *enhanced measures* necessary in accordance with Paragraph 5(2) of *Schedule 3*.

48. Where the firm identifies that a *foreign PEP* is a director (or equivalent) of a *customer*, or a person acting or purporting to act for a *customer*, but where the *PEP* does not fall within the definition of *beneficial owner* and where no *funds* or assets of that *PEP* are handled in the particular *business relationship* or *occasional transaction*, the firm should include as part of its

relationship risk assessment consideration of the nature of the *PEP's* role and the reason why the *PEP* holds such a role.

49. Where the firm has determined as part of its *relationship risk assessment* that, but for the function held by the *PEP* in the circumstances in Paragraph 8.48. above, the *business relationship* or *occasional transaction* would be other than high *risk*, it could decide to apply, based on *risk*, *CDD* measures appropriate to the form of the *customer* in accordance with Chapters 4 to 9 of this *Handbook*, including *enhanced measures* as applicable.

50. One such example would be a *foreign* public sector pension scheme investing into a CIS. In such a case there may be members of the pension committee who are *PEPs*, holding their position on the committee by virtue of their political position and with no ability to exercise ultimate effective control over the pension scheme. Such persons have no economic interest in the *funds* involved in the *business relationship* or *occasional transaction* (beyond potentially any pension rights as a resident of that country or organisation) and the *risk* of the relationship being used as a vehicle for the laundering of any *funds* or assets personally held by the *PEP* or the financing of terrorism or proliferation is low.

8.5.3. International Organisation PEPs

51. In accordance with Paragraph 5(4)(b) of *Schedule 3*, the definition of a *PEP* includes a natural person who is, or has been, entrusted with a prominent public function by an *international organisation*. This includes members of senior management or individuals who have been entrusted with equivalent functions, for example, directors, councillors and members of the board or equivalent of an *international organisation*.

52. Paragraph 21 of *Schedule 3* defines an *international organisation* as an entity:

(a) which was established by a formal political agreement between its member states that has the status of an international treaty;
(b) the existence of which is recognised by law in its member states; and
(c) which is not treated as a resident institutional unit of the country in which it is located.

53. Examples of *international organisations* covered by *Schedule 3* and this *Handbook* include the UN, the World Bank and the North Atlantic Treaty Organization ("NATO").

54. There may be other examples of *international organisations*, for example, international sporting federations, which do not fall within the *Schedule 3* definition, but where the firm considers that *ECDD* measures should be applied to a *business relationship* or *occasional transaction*. There are no prescribed requirements in this regard and any decision taken should be based on the firm's assessment of *risk*.

8.5.4. Immediate Family Members

55. In addition to the specific *risks* posed by *PEPs*, the firm should be alive to the potential for the abuse of a *business relationship* or *occasional transaction* with or by a family member of a *PEP*. This abuse could be for the purpose of moving the *proceeds* of crime or facilitating the placement and concealment of such *proceeds* without specific connection to the *PEP* themselves.

56. In accordance with Paragraph 5(4)(c) of *Schedule 3*, an immediate family member of a *PEP* shall include, without limitation:

(a) a spouse;
(b) a partner, being a person who is considered by the law of the country or territory in which the relevant public function is held as being equivalent to a spouse;

(c) a parent;
(d) a child;
(e) a sibling;
(f) a parent-in-law; and
(g) a grandchild.

57. The list of immediate family members included within Paragraph 5(4)(c) of *Schedule 3* as set out above is without limitation and the firm should take a proportionate, *risk*-based approach to the treatment of wider family members. This determination will depend on the social, economic and cultural structure of the country of the *PEP*. It should also be noted that the number of persons who qualify as immediate family members is fluid and may change over time.

58. In deciding whether a member of a wider family unit would be considered as an immediate family member of a *PEP*, the firm should determine the extent of the influence that a particular *PEP* relationship or association has and assess the level of *risk* that exists through the particular connection with a *PEP*.

59. This determination will include such relevant factors as the influence that particular types of family members generally have and how broad the circle of close family members and dependents tends to be. In some cultures the number of family members who are considered to be close or who have influence may be quite small, while in others the circle of family members may be broader and extend to cousins or even clans.

8.5.5. Close Associates

60. In accordance with Paragraph 5(4)(d) of *Schedule 3*, a close associate of a person referred to in Paragraphs 5(4)(a) or (b) shall include, without limitation -

(i) a person who is widely known to maintain a close business relationship with such a person, or
(ii) a person who is in a position to conduct substantial financial transactions on behalf such a person.

61. Those persons considered to be close associates could include known partners outside the family unit who would not qualify as immediate family members (for example, girlfriends, boyfriends and extra-marital partners), prominent members of the same political party, civil organisation, labour or employee union as the *PEP*, and business partners or associates, especially those that share beneficial ownership of a *legal person* or *legal arrangement* with the *PEP*, or who are otherwise connected (for example, through joint membership of a company board where the *PEP* and/or close associate is a *beneficial owner*).

62. As with an immediate family member, the interpretation of whether an individual should be considered to be a close associate will depend upon the social, economic and cultural context of the relationship.

63. Where the firm determines that a natural person who is the *customer* or *beneficial owner* to a *business relationship* or *occasional transaction* is an immediate family member or close associate of a *domestic PEP* or *international organisation PEP*, the firm should treat that person in accordance with the requirements set out in *Schedule 3* and this *Handbook* for the category of *PEP* to which they are connected. For example, the child of a *domestic PEP* should be treated in accordance with the provisions for *domestic PEPs*.

8.5.6. Former PEPs

64. On the basis of the potential for *PEPs* to abuse their prominent positions for the purpose of committing various financial crimes, the default position on the treatment of *PEPs* in *the FATF Recommendations* is that once you are a *foreign PEP*, or a family member or close associate of such a person, the relationship should always be subject to *ECDD* measures.

65. Notwithstanding the above, there may be situations where a *business relationship* or *occasional transaction* involves persons who have held prominent public positions historically but who would otherwise not be considered to be high *risk*.

66. Accordingly, Paragraph 5 of *Schedule 3* provides flexibility in respect of the timeframe within which certain natural persons are to be classified as *PEPs*. Details of these timeframes are included within Sections 8.5.6.1. to 8.5.6.3. of this *Handbook* below and differ depending on the type of *PEP* and the position that the *PEP* holds.

Category of PEP	Role of PEP	Time Period for Declassification
Foreign PEP	A head of state or head of government (or an immediate family member or close associate of such a person).	Never
	A person with the power to direct the spending of significant sums (or an immediate family member or close associate of such a person).	Never
	All other *foreign PEPs* (including immediate family members and close associates thereof).	7 years from cessation of role
International Organisation PEP	A head of an *international organisation* (or an immediate family member or close associate of such a person).	Never
	A person with the power to direct the spending of significant sums (or an immediate family member or close associate of such a person).	Never
	All other *international organisation PEPs* (including immediate family members and close associates thereof).	7 years from cessation of role
Domestic PEP	All *domestic PEPs* (including immediate family members and close associates thereof).	5 years from cessation of role

Fig. 12 - Timescales for Declassification PEPs

67. Details on the requirements of *Schedule 3*, together with additional *guidance*, are provided within the following sections setting out the steps to be taken by the firm when it is looking to establish a *business relationship* or undertake an *occasional transaction* within which the *customer* or *beneficial owner* is a former *PEP*.

68. In accordance with Paragraph 5(8) of *Schedule 3* (and as reflected in Fig. 12 above), the measures set out in Sections 8.5.6.1. - 8.5.6.3. below apply in respect of persons falling within Paragraphs 5(4)(c)-(d) of *Schedule 3* (immediate family members and close associates) in respect of the person in question as they do in respect of that person.

8.5.6.1. Domestic PEPs, Family Members and Close Associates

69. In accordance with Paragraph 5(5) of *Schedule 3*, the firm may treat a *domestic PEP* as not being a PEP five years after the person ceased to be entrusted with a public function (for the purposes of this *Handbook*, a "former *domestic PEP*") if the senior management of the firm has documented that the firm is satisfied that –

(a) it understands the source of the *funds* within the *business relationship* or *occasional transaction*, and
(b) there is no reason to continue to treat the person as a *PEP*.

70. For any natural person falling within Paragraph 5(5) of *Schedule 3*, the firm can make a decision to declassify that person as a *domestic PEP* following a period of five years, such period commencing on the date that they, or the associated *domestic PEP* in the case of an immediate family member or close associate, ceased to be entrusted with any prominent public function within *the Bailiwick*.

71. Where, during the course of a *business relationship* (or in the case of a prospective *business relationship* or *occasional transaction*, prior to the firm being engaged), the *customer* or *beneficial owner* becomes a former *domestic PEP*, consideration of their previous function as part of a *relationship risk assessment* in accordance with *Commission Rule* 8.45. is not required, provided that the criteria in Paragraph 8.69. above are met.

72. Where the firm identifies, in accordance with Paragraph 4(3)(f) of *Schedule 3*, that the *customer* to a prospective *business relationship* or *occasional transaction*, or any *beneficial owner* of such, has held a prominent public function within *the Bailiwick* within the past five years, the firm should consider this as a factor when undertaking its *relationship risk assessment* in accordance with *Commission Rule* 8.45. above.

8.5.6.2. International Organisation PEPs, Family Members and Close Associates

73. In accordance with Paragraph 5(6) of *Schedule 3*, subject to Paragraph 5(9), the firm may treat an *international organisation PEP* as not being such a *PEP* seven years after the person ceased to be entrusted with a prominent function by an *international organisation* if the senior management of the firm has documented that the firm is satisfied that -

(a) it understands the source of the *funds* within the *business relationship* or *occasional transaction*, and
(b) there is no reason to continue to treat the person as a *PEP*.

74. In accordance with Paragraph 5(9) of *Schedule 3*, the provisions set out in Paragraph 8.73. above do not apply in respect of -

(a) a head of an *international organisation*,
(b) a person with the power to direct the spending of significant sums, or
(c) persons falling within Paragraphs 5(4)(c)-(d) of *Schedule 3* (immediate family members and close associates) in respect of such persons.

75. In determining whether an *international organisation PEP* falls within Paragraph 8.74.(b) above, the firm should consider whether:

(a) the *international organisation PEP* has/had authority over, or access to, significant assets and *funds*, policies and/or operations of the *international organisation*;
(b) the *international organisation PEP* has/had access to, or control or influence over, the *accounts* of the *international organisation*; and
(c) the *international organisation PEP* has/had control over the awarding of contracts or similar by the *international organisation*.

76. For any other natural person falling within Paragraph 5(4)(b) of *Schedule 3*, the firm can make a decision to declassify that person as an *international organisation PEP* following a period of seven years, such period commencing on the date that they, or the associated *international*

organisation PEP in the case of an immediate family member or close associate, ceased to be entrusted with any prominent public function (a "former *international organisation PEP*").

77. Where, during the course of a *business relationship* (or in the case of a prospective *business relationship* or *occasional transaction*, prior to the firm being engaged) the *customer* or *beneficial owner* becomes a former *international organisation PEP*, consideration of their previous function as part of a *relationship risk assessment* in accordance with *Commission Rule* 8.45. is not required, provided that the criteria in Paragraph 5(6) of *Schedule 3* are met.

78. Where the firm identifies, in accordance with Paragraph 4(3)(f) of *Schedule 3*, that the *customer* or *beneficial owner* to a prospective *business relationship* or *occasional transaction* has held a prominent public function with an *international organisation* within the past seven years, the firm should consider this as a factor when undertaking its *relationship risk assessment* in accordance with *Commission Rule* 8.45. above.

8.5.6.3. Foreign PEPs, Family Members and Close Associates

79. In accordance with Paragraph 5(7) of *Schedule 3*, subject to Paragraph 5(9), the firm may treat any *foreign PEP* as not being a *PEP* seven years after the person ceased to be entrusted with a public function if the senior management of the firm has documented that the firm is satisfied that -

    (a) it has established and understands the source of the person's wealth, and that of the *funds* within the *business relationship* or *occasional transaction*, and
    (b) there is no reason to continue to treat the person as a *PEP*.

80. In accordance with Paragraph 5(9) of *Schedule 3*, the provisions set out in Paragraph 8.79. above do not apply in respect of -

    (a) a head of state or head of government,
    (b) a person with the power to direct the spending of significant sums, or
    (c) persons falling within Paragraphs 5(4)(c)-(d) of *Schedule 3* (immediate family members and close associates) in respect of such persons.

81. In determining whether a *foreign PEP* falls within Paragraph 8.80.(b) above, the firm should consider whether:

    (a) the *foreign PEP* has/had access to, or authority, control or influence over, significant state assets and *funds*, policies and/or operations;
    (b) the *foreign PEP* has/had control over regulatory approvals, including awarding licences and concessions;
    (c) the *foreign PEP* has/had the formal or informal ability to control mechanisms established to prevent and detect *ML*, *TF* and/or *PF* (for example, control over law enforcement or other public sector investigative agencies); and
    (d) the *foreign PEP* has/had access to, or authority, control or influence over, the assets of state owned enterprises.

82. For all other *foreign PEPs* falling within Paragraph 5(4)(a) of *Schedule 3*, the firm could decide to declassify a natural person as a *foreign PEP* following a period of seven years, such period commencing on the date that they, or the associated *foreign PEP* in the case of an immediate family member or close associate, ceased to be entrusted with any prominent public function (a "former *foreign PEP*").

83. Where, during the course of a *business relationship* (or in the case of a prospective *business relationship* or *occasional transaction*, prior to the firm being engaged) the *customer* or *beneficial owner* becomes a former *foreign PEP*, the firm is not required to apply the measures

set out in Paragraph 8.44. of this *Handbook* for that natural person provided that the criteria in Paragraph 5(7) of *Schedule 3* are met.

84. Where the firm identifies, in accordance with Paragraph 4(3)(f) of *Schedule 3*, that the *customer* or *beneficial owner* to a prospective *business relationship* or *occasional transaction* has held a prominent public function outside *the Bailiwick* within the past seven years, it should continue to treat that individual as a *foreign PEP* in accordance with the requirements of Paragraph 5 of *Schedule 3* and Section 8.5.2. of this *Handbook*.

8.6. Correspondent Relationships

85. Correspondent banking is the provision of banking services by one *bank* to another *bank* ("the respondent *bank*"). Used by *banks* throughout the world, correspondent *accounts* enable *banks* to conduct business and provide services that they do not offer directly. There are also similar relationships in other areas of *financial services business*.

86. In accordance with Paragraph 5(1)(b) of *Schedule 3*, the firm shall apply *ECDD* measures in relation to a *business relationship* or *occasional transaction* which is a *correspondent banking relationship*, or similar to such a relationship in that it involves the provision of services, which themselves amount to *financial services business* or facilitate the carrying on of such business, by one *financial services business* to another.

87. Additionally, in accordance with Paragraph 8(2) of *Schedule 3*, the firm shall:

(a) not enter into, or continue, a *correspondent banking relationship* with a *shell bank*; and
(b) take appropriate measures to ensure that it does not enter into, or continue, a *correspondent banking relationship* where the respondent *bank* is known to permit its *accounts* to be used by a *shell bank*.

88. In relation to *correspondent banking relationships* and similar correspondent relationships established for securities transactions or *funds* transfers, whether for the firm as principal or for its *customers*, the firm must apply the measures set out in (a) to (e) below and, where relevant, those in *Commission Rule* 8.89. below:

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent institution's business;
(b) determine from publicly available information the reputation of the respondent institution and the quality of supervision, including whether it has been subject to an *ML, TF* or *PF* investigation or regulatory action;
(c) assess the respondent institution's AML and CFT policies, procedures and controls and ascertain that they are adequate, appropriate and effective;
(d) obtain *board* approval before establishing new correspondent relationships; and
(e) clearly understand and *document* the respective AML, CFT and CPF responsibilities of each institution.

89. Where a correspondent relationship involves the maintenance of 'payable-through *accounts'*, the firm must also take steps in order to *satisfy* itself that:

(a) the *customer* (the respondent institution) has complied with all of the required *CDD* measures set out in *Schedule 3* and this *Handbook* on those of its *customers* with direct access to the *accounts* of the correspondent institution; and
(b) the respondent institution is able to provide relevant *CDD information* upon request to the correspondent institution.

90. The firm must ensure that appropriate and effective policies, procedures and controls are in place when establishing a correspondent relationship with a foreign *bank* or other *financial services business*.

91. Additionally, the firm must have appropriate and effective policies, procedures and controls in place to ensure compliance with the requirements of Paragraph 8 of *Schedule 3* in respect of *shell banks*.

8.7. High Risk Countries and Territories

92. In accordance with Paragraph 5(1)(c)(i) of *Schedule 3*, the firm shall apply *ECDD* measures to a *business relationship* or *occasional transaction* where the *customer* or *beneficial owner* has a *relevant connection* with a country or territory that -

(A) provides funding or support for terrorist activities, or does not apply (or insufficiently applies) *the FATF Recommendations*, or
(B) is a country otherwise identified by the FATF as a country for which such measures are appropriate.

93. For the purposes of Paragraph 5(1)(c), Paragraph 5(10) of *Schedule 3* defines that a *customer* or *beneficial owner* has a '*relevant connection*' with a country or territory if the *customer* or *beneficial owner* –

(a) is the government, or a public authority, of the country or territory,
(b) is a *PEP* within the meaning of Paragraph 5(4) of *Schedule 3* in respect of the country or territory,
(c) is resident in the country or territory,
(d) has a business address in the country or territory,
(e) derives *funds* from –

(i) assets held by the *customer* or *beneficial owner*, or on behalf of the *customer* or *beneficial owner*, in the country or territory, or
(ii) income arising in the country or territory, or

(f) has any other connection with the country or territory which the firm considers, in light of the firm's duties under *Schedule 3* (including but not limited to its duties under Paragraph 2 of *Schedule 3*), to be a *relevant connection* for those purposes.

94. The firm must have policies, procedures and controls in place which enable it to determine those countries or territories falling within Paragraph 5(1)(c)(i) of *Schedule 3*.

95. The FATF regularly updates its public statement, "High Risk Jurisdictions subject to a Call for Action" in which it calls on all members and urges all jurisdictions to apply enhanced due diligence, and in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the ongoing *ML*, *TF*, and *PF risks* emanating from the country. This list is often externally referred to as the "black list". For the purposes of applying Paragraph 5(1)(c)(i) of *Schedule 3*, Appendix H to this *Handbook* identifies those countries and territories which the FATF has listed as high *risk*.

96. As part of its policies, procedures and controls, the firm must:

(a) be aware of concerns about weaknesses in the AML, CFT and CPF systems of other countries or territories; and

(b) consider any updates to Appendix H of this *Handbook* and Notices, Instructions and Warnings issued from time to time by *the Commission*.

8.8. Bearer Shares and Bearer Warrants

97. In accordance with Paragraph 5(1)(e) of *Schedule 3*, the firm shall apply *ECDD* measures to a *business relationship* or *occasional transaction* in which the *customer*, the *beneficial owner* of the *customer*, or any other *legal person* in the ownership and control structure of the *customer*, is a *legal person* that has *bearer shares* or *bearer warrants*.

98. A *bearer share* is a share that is owned by, and gives all associated rights to, the person who is in control or possession of the share. The *bearer share* is not recorded by indefeasible title (for example, on a register) and transfer of the ownership of the share does not need to go through a register to be effected. As there are no records as to the holder, it is often difficult to identify the true or ultimate *beneficial owner* of a *bearer share*, or more broadly, *bearer share* companies.

99. Where the firm's *risk appetite* allows for a *customer*, the *beneficial owner* of a *customer*, or any other *legal person* in the ownership and control structure of the *customer* to have *bearer shares* and/or *bearer warrants*, the firm must have appropriate and effective policies, procedures and controls in place to mitigate the *risk* posed by their use.

100. Where the firm establishes or maintains a *business relationship* or undertakes an *occasional transaction* falling within Paragraph 5(1)(e) of *Schedule 3*, the firm must apply both of the following measures in respect of that *business relationship* or *occasional transaction*, together with the *ECDD* measures set out in Paragraph 5(1) of *Schedule 3*:

(a) determine and satisfy itself as to the reasons why the *customer*, the *beneficial owner* of the *customer*, or other *legal person* in the ownership and control structure of the *customer* has *bearer shares* and/or *bearer warrants*; and
(b) have custody of the *bearer shares* and/or *bearer warrants*, or be satisfied as to their location and immobilisation. This should include confirming the number and location of the *bearer shares* and/or *bearer warrants* on a periodic basis, or alternatively, receiving a written undertaking from the custodian of those *bearer shares* and/or *bearer warrants* that the firm will be notified of any changes to records relating to them and their custodian.

101. The firm must apply the above policies, procedures and controls to a *business relationship* or *occasional transaction* irrespective of whether the identified *bearer share* or *bearer warrant* represents an amount below the relevant threshold for ownership or control of the *legal person*.

Enhanced Measures

102. In accordance with Paragraph 5(2) of *Schedule 3*, the firm shall carry out *enhanced measures* in relation to *business relationships* and *occasional transactions*, whether otherwise high *risk* or not, which involve or are in relation to -

(a) a *customer* who is not resident in *the Bailiwick*;
(b) the provision of private banking services;
(c) a *customer* which is a *legal person* or *legal arrangement* used for personal asset holding purposes; or
(d) a *customer* which is –

(i) a *legal person* with *nominee shareholders*, or
(ii) owned by a *legal person* with *nominee shareholders*.

103. Paragraphs 5(3)(b) and 16A of *Schedule 3* defines *enhanced measures* as being the carrying out of appropriate and adequate enhanced measures in relation to a *business relationship* or *occasional transaction*, to mitigate and manage the specific higher *risk* of *ML, TF* and *PF* resulting from the matters listed in Paragraph 5(2) of *Schedule 3* that are relevant to that relationship or transaction.

104. For a number of *business relationships* or *occasional transactions* there is likely to be more than one *specified business* involved and the firm should be aware that the *enhanced measures* it applies may be different to those applied by another *specified business* to mitigate differing higher *risk* factors.

105. By way of example, a fiduciary establishes a trust for a non-resident *customer* to whom it applies *enhanced measures* as set out in Section 8.9. below. The fiduciary then acts as the *customer* in a *business relationship* with another *specified business* where, acting as trustee, it opens a *bank account* on behalf of the trust with a private *bank*. The *bank* will apply *enhanced measures* to mitigate the higher *risks* associated with its *customer* being a personal asset holding vehicle and the provision of private banking services as detailed in Sections 8.10. and 8.11., which may be different to those applied by the fiduciary.

8.9. Non-Resident Customer

106. *Customers* who are not resident in a country or territory but who nevertheless seek to form a *business relationship* or conduct an *occasional transaction* with a business in that country or territory will generally have legitimate reasons for doing so. However, some such *customers* may present a higher *risk* of *ML, TF* and/or *PF*, for example, by attempting to move illicit *funds* away from their country or territory of residence or attempting to further conceal the source of *funds* from that country or territory.

107. For the purposes of Paragraph 5(2)(a) of *Schedule 3*, examples of *enhanced measures* the firm could apply in respect of a *business relationship* or *occasional transaction* involving or in relation to a *customer* who is not resident in *the Bailiwick* could include:

(a) taking steps to understand the reason(s) behind the *customer* seeking to establish a *business relationship* or carry out an *occasional transaction* with the firm;
(b) the use of external data sources to collect information on the *customer* and the particular country *risk* in order to build a *customer* business and *risk* profile similar to that available for a resident *customer*;
(c) taking reasonable measures to establish and understand the source of the *funds* used within the *business relationship* or *occasional transaction* and considering whether this is consistent with the firm's understanding of the *customer* and the rationale for the *business relationship* or *occasional transaction* (see Section 8.3. of this *Handbook*).

108. For the purposes of Paragraph 8.107.(a), when determining the reasons for establishing a *business relationship* or undertaking an *occasional transaction*, the firm should *document* its determination. The reasons given should be more detailed and substantive than merely 'tax planning', 'asset protection' or similar.

109. Where the firm determines that the rationale for the *customer* establishing a *business relationship* or undertaking an *occasional transaction* with the firm is tax planning or tax mitigation, the firm should seek to understand the underlying tax rationale for the *business relationship* or *occasional transaction*. Where concerns are raised about this rationale, the firm could consider requesting a copy of the tax opinion or tax advice to support its understanding of the *customer's* arrangements.

110. With regard to Paragraph 8.107.(c) above, when seeking to establish the source of any *funds*, the firm should consider both the activities which generated those *funds* in order to understand the provenance of the *funds* and any potential implications to those *funds* being moved to *the*

Bailiwick. For example, is the *customer* seeking to circumvent capital controls by moving the *funds* to the firm.

8.10. Customer Provided with Private Banking Services

111. Private banking is generally understood to be the provision of personalised banking and/or investment services to high-net-worth *customers* in a closely managed relationship. It may involve complex, bespoke arrangements and high value transactions across multiple countries and territories. Such *customers* may therefore present a higher *risk* of *ML, TF* and/or *PF*.

112. For the purposes of this Section a service is regarded as a private banking service if it meets all four of the following criteria:

(a) is offered or proposed to personal, private client, *customers* (either directly or through a *legal person* or *legal arrangement*) identified by the firm as being eligible for the service on the basis of their net worth;
(b) involves high value investment;
(c) is non-standardised; and
(d) is tailored to the *customer's* needs.

113. For the avoidance of doubt, private banking services are not considered to be solely the preserve of a *bank* (with the exception of accepting deposits) but could feasibly be offered by a firm licensed under *the POI Law*. A business licensed under *the Fiduciaries Law* who facilitates private banking services as part of its duties as a trustee is not considered to be providing private banking services.

114. For the purposes of Paragraph 5(2)(b) of *Schedule 3*, examples of *enhanced measures* the firm could apply in respect of a *business relationship* or *occasional transaction* involving or in relation to the provision of private banking services could include:

(a) reviewing the *business relationship* more frequently, including all *documents*, data and information obtained as part of the firm's *CDD* measures in order to ensure that they continue to be appropriate and relevant;
(b) where transaction monitoring thresholds are used, ensuring that these are appropriate for the circumstances of the *business relationship* and considering whether they should be reduced to provide greater oversight of transactions connected with the *business relationship*;
(c) taking reasonable measures to establish and understand the source of any *funds* and of the wealth of the *customer* and *beneficial owner* (see Section 8.3. of this *Handbook*).

115. Where the firm offers private banking services alongside other corporate or retail services, it should consider on a case by case basis whether a *customer* utilises such private banking services, taking into account Paragraph 8.112. above, or whether the products and/or services provided to the *customer* fall within more traditional retail banking services. If the latter, there is no requirement to apply the *enhanced measures* set out above.

8.11. Customer is a Personal Asset Holding Vehicle

116. Personal asset holding vehicles are *legal persons* or *legal arrangements* established by natural persons for the specific purpose of holding assets for investment. Whilst there are some perfectly legitimate reasons for establishing a personal asset holding vehicle, the use of such, either a *legal person* or *legal arrangement*, can serve to conceal the true source of wealth and *funds*, or the identity of the ultimate *beneficial owner* of the investment. The use of personal asset holding

vehicles therefore presents a higher *risk*, making it more difficult for the firm to establish the true beneficial ownership of a *customer*.

117. Notwithstanding the above, the extent of the *risk* associated with the personal asset holding vehicle could vary depending upon whether a regulated trust and corporate service provider is providing corporate services to the personal asset holding vehicle. This will in turn determine the extent of the *enhanced measures* to be applied by the firm to the *customer*.

118. For the purposes of Paragraph 5(2)(c) of *Schedule 3*, examples of *enhanced measures* the firm could apply in respect of a *business relationship* or *occasional transaction* involving or in relation to a *customer* which is a *legal person* or *legal arrangement* used for personal asset holding purposes could include:

(a) determining the purpose and rationale for making use of a personal asset holding vehicle rather than a *beneficial owner* holding assets in their own name and *satisfying* itself that the use of such a vehicle has a genuine and legitimate purpose;
(b) taking reasonable measures to establish and understand the source of any *funds* and of the wealth of the *customer* and *beneficial owner* (see Section 8.3. of this *Handbook*).

119. Paragraph 5(2)(c) applies where the personal asset holding vehicle is the *customer* or the third party where the *customer* is a trustee or general partner acting on behalf of a personal asset holding vehicle.

120. For the purposes of Paragraph 8.118.(a) above, when determining the purpose and rationale for the use of an asset holding vehicle, the firm should *document* its determination. The reasons given should be more detailed and substantive than merely 'tax planning', 'asset protection' or similar.

121. Where the firm determines that the rationale for the *customer* making use of a personal asset holding vehicle is tax planning or tax mitigation, the firm should seek to understand the underlying tax rationale. Where concerns are raised about this rationale, the firm could consider requesting a copy of the tax opinion or tax advice to support its understanding of the *customer's* arrangements.

8.12. Customer with Nominee Shareholders

122. There may be sound commercial reasons for a *customer* using *nominee shareholders*, for example, to ease administration and reduce costs by tasking the nominee to undertake essential corporate actions in the administration of the structure.

123. Notwithstanding the above, as detailed in Section 7.3. of this *Handbook*, the use of *nominee shareholders* can provide a *customer* with the means to obscure true ownership and control by separating legal and beneficial ownership. The use of *nominee shareholders* therefore presents a higher *risk*, making it more difficult for the firm to establish the true beneficial ownership of a *customer*.

124. For the purposes of Paragraph 5(2)(d) of *Schedule 3*, examples of *enhanced measures* the firm could apply in respect of a *business relationship* or *occasional transaction* involving or in relation to a *customer* which is a *legal person* with *nominee shareholders*, or owned by a *legal person* with *nominee shareholders*, could include:

(a) determining and satisfying itself as to the reasons why the *customer*, or a *legal person* which owns the *customer*, is making use of *nominee shareholders*;
(b) using external data sources to collect information on the fitness and propriety of the *nominee shareholder* (such as their regulated status and reputation) and the particular country *risk*;

(c) where nominees are used in *intermediary relationships* falling within Section 9.8. of this *Handbook*, the measures the firm must take in accordance with the *Commission Rules* in Section 9.8.2.

Where the firm enters into a *business relationship* or undertakes an *occasional transaction* with a CIS which is authorised or registered by *the Commission* and has not been nominated as the party responsible for applying *CDD* measures to investors in that CIS in accordance with Section 4.8.1. of this *Handbook*, it is not required to apply *enhanced measures* in respect of that CIS where the CIS has *nominee shareholders*, for example, an *intermediary* investing into the CIS on behalf its own customers.

Chapter 9
Simplified Customer Due Diligence

Contents of this Chapter

9.1. Introduction

1. This Chapter provides for the treatment of *business relationships* and *occasional transactions* which have been assessed as being *low risk relationships* pursuant to Paragraph 3 of *Schedule 3* and Chapter 3 of this *Handbook*. It sets out the ability to apply *SCDD* measures to *business relationships* or *occasional transactions* in specific circumstances and defines those simplified measures which can be applied.

2. This Chapter should also be read in conjunction with Chapters 4 to 7 of this *Handbook* which provide for the overarching *CDD* obligations and the specific requirements for the differing categories of natural persons, *legal persons* and *legal arrangements* with which the firm could deal as part of a *business relationship* or *occasional transaction*.

9.2. Simplified Customer Due Diligence Measures

3. The general rule is that *business relationships* and *occasional transactions* are subject to the full range of *CDD* measures as set out in *Schedule 3* and this *Handbook*, including the requirement to identify and verify the identity of the *customer* and to identify and take reasonable measures to verify the identity of the *beneficial owner*.

4. However, there may be circumstances where the *risks* of *ML, TF* and *PF* have been assessed by the firm as being low. Examples could include:

   (a) a *Bailiwick* resident *customer* where the purpose and intended nature of the *business relationship* or *occasional transaction* is clearly understood by the firm;
   (b) a *business relationship* or *occasional transaction* where the *risks* associated with the relationship are inherently low and information on the identity of the *customer* and *beneficial owner* is publicly available, or where adequate checks and controls exist elsewhere in publicly available systems; or
   (c) a *business relationship* or *occasional transaction* in which the *customer* is an *Appendix C business*.

5. There may also be circumstances where the *risk* of *ML, TF* and *PF* has been assessed as low by *the Bailiwick* as part of its *NRA*. In these circumstances, the firm may consider applying *SCDD* measures when identifying, and verifying the identity of, the *customer* and *beneficial owner*.

National Risk Assessment

6. In accordance with Paragraph 6(1) of *Schedule 3*, where the firm is required to carry out *CDD* in relation to a *business relationship* or *occasional transaction* which has been assessed as a *low risk relationship* pursuant to Paragraph 3(4)(a) or in accordance with the *NRA*, it may, subject to the provisions of Paragraphs 6(2) and 6(3) of *Schedule 3*, apply reduced or *SCDD* measures.

7. In accordance with Paragraph 6(2) of *Schedule 3*, the discretion in Paragraph 6(1) as set out above may only be exercised by the firm:

   (a) in accordance with the requirements set out in this *Handbook*, and
   (b) where it complies with the requirements of Paragraph 3 of *Schedule 3*.

8. The *SCDD* measures applied by the firm should be commensurate with the low *risk* factors and should relate only to relationship acceptance measures or to aspects of ongoing monitoring (excluding sanctions screening). Examples of possible measures could include:

(a) reducing the verification measures applied to the *customer* and/or *beneficial owner*, in accordance with the following sections of this Chapter;
(b) reducing the degree of on-going monitoring and scrutiny of transactions, based on a reasonable monetary threshold; or
(c) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the *business relationship* or *occasional transaction*, but inferring the purpose and nature from the type of transaction(s) or *business relationship* established.

9. The firm must ensure that, when it becomes aware of circumstances which affect the assessed *risk* of a *business relationship* or *occasional transaction* to which *SCDD* measures have been applied, a review of the *relationship risk assessment* is undertaken and a determination is made as to whether the *identification data* held remains appropriate to the revised *risk* of the *business relationship* or *occasional transaction*.

10. Where the firm has taken a decision to apply *SCDD* measures, documentary evidence must be retained which reflects the reason for the decision. The *documentation* retained must provide justification for the decision, including why it is deemed acceptable to apply *SCDD* measures having regard to the circumstances of the *business relationship* or *occasional transaction* and the *risks* of *ML, TF* and *PF*.

11. In accordance with Paragraphs 6(3) and 16A of *Schedule 3*, for the avoidance of doubt, the discretion to apply *SCDD* measures shall not be exercised:

(a) where the firm forms a suspicion that any party to a *business relationship* or *occasional transaction* or any *beneficial owner* is or has been engaged in *ML, TF* or *PF*, or
(b) in relation to a *business relationship* or *occasional transaction* where the *risk* is other than low.

9.3. Bailiwick Residents

12. Where the *customer*, *beneficial owner* or other *key principal* to a *business relationship* or *occasional transaction* is a natural person resident in *the Bailiwick*, the firm may apply *SCDD* measures in respect of that natural person, provided the requirements as set out in Section 9.2. above are met. Where the firm has determined that it can apply *SCDD* measures because the *risk* has been assessed as low, it may elect to verify one of points (b) date of birth and (c) residential address under *Commission Rule* 5.8., in addition to (a) legal name.

13. Notwithstanding the above, it should be borne in mind that not all *Bailiwick* residents are intrinsically low *risk*. The firm must ensure that a *relationship risk assessment* is undertaken in accordance with the requirements of Paragraph 3 of *Schedule 3* and Chapter 3 of this *Handbook* and that where the *business relationship* or *occasional transaction* is considered to be other than low *risk*, that the appropriate *CDD*, and where necessary *ECDD*, measures are applied.

9.4. Bailiwick Public Authorities

14. Where the *customer*, *beneficial owner* or other *key principal* to a *business relationship* or *occasional transaction* has been identified as a *Bailiwick* public authority, the firm may choose to apply *SCDD* measures in respect of that public authority. Where *SCDD* measures are applied, it is not necessary for the firm to apply full verification measures to the public authority (and the *beneficial owners* thereof), other than where the firm considers this course of action appropriate in the circumstances.

15. The firm must identify, and verify the identity of, *the Bailiwick* public authority, including as a minimum:

(a) the full name of the public authority;
(b) the nature and status of the public authority;
(c) the address of the public authority; and
(d) the names of the directors (or equivalent) of the public authority.

16. The following are examples of *Bailiwick* public authorities:

(a) a government department;
(b) an agency established by law;
(c) a parish authority/douzaine; and
(d) a body majority owned by an authority listed in points (a) to (c) above.

17. Where a natural person authorised to act on behalf of a *Bailiwick* public authority is acting in the course of employment, it is not necessary to identify and verify the identity of that person. However, the firm should verify the natural person's authority to so act.

18. It may be that an individual acting on behalf of a *Bailiwick* public authority falls within the definition of a *domestic PEP*. However, in the context of acting for *the Bailiwick* public authority, the individual is directing funds belonging to the authority and not their personal funds. The firm may therefore determine that the measures required under *Commission Rule* 9.15. are sufficient and that the prominent public function held by the natural person does not pose an increased *risk* to the firm in the context of the *business relationship* or *occasional transaction* with *the Bailiwick* public authority.

9.5. Collective Investment Schemes Authorised or Registered by the Commission

19. Where the *customer*, *beneficial owner* or other *key principal* to a *business relationship* or *occasional transaction* is a CIS authorised or registered by *the Commission*, the firm (other than where it has been nominated as the party responsible for applying *CDD* measures to investors in accordance with Section 4.8.1. of this *Handbook*) may consider the CIS to be the principal for the purposes of the firm's *CDD* measures.

20. Where this is the case, in verifying the identity of the CIS the firm must, as a minimum, obtain *documentation* which confirms the CIS is authorised or registered by *the Commission*.

21. Further information about CISs authorised and registered by *the Commission* can be found on *the Commission's* website:

https://www.gfsc.gg/industry-sectors/investment/regulated-entities

22. Where a natural person authorised to act on behalf of a CIS to which this Section applies is doing so in the course of employment with that CIS or its Designated Manager, it is not necessary to identify and verify the identity of that person. However, the firm should verify the person's authority to act on behalf of the CIS.

23. As an example, where a *bank* is opening an *account* for a CIS authorised or registered by *the Commission*, the *bank* may treat the CIS as the *customer* to be identified and verified.

9.6. Appendix C Businesses

24. Appendix C to this *Handbook* lists those countries or territories which *the Commission* considers require regulated *FSBs*, and in limited circumstances *PBs*, to have in place measures consistent with *the FATF Recommendations* and where such businesses are appropriately supervised for compliance with those requirements. Appendix C is reviewed periodically with countries or territories being added or removed as appropriate.

25. The fact that a country or territory has requirements that are consistent with *the FATF Recommendations* means only that the necessary legislation and other means of ensuring compliance with *the FATF Recommendations* are in force in that country or territory. It does not provide assurance that a particular overseas business is subject to that legislation, or that it has implemented the necessary measures to ensure compliance with that legislation.

26. The inclusion of a country or territory in Appendix C does not mean that the country or territory in question is intrinsically low *risk*, nor does it mean that any *business relationship* or *occasional transaction* in which the *customer* or *beneficial owner* has a connection to such a country is to be automatically treated as a *low risk relationship*.

27. Where the *customer* has been identified as an *Appendix C business* and the purpose and intended nature of the *business relationship* or *occasional transaction* is understood, subject to *Commission Rule* 9.28. and with the exception of the circumstances set out in Paragraph 9.31. below, verification of the identity of the *Appendix C business* is not required.

28. With the exception of the provisions in Sections 9.8. and 9.9. of this Chapter, if the *Appendix C business* is acting for or on behalf of another party the firm must, in accordance with Paragraph 4(3)(d) of *Schedule 3*, take reasonable measures to identify and verify the identity of that third party in accordance with the requirements of *Schedule 3* and this *Handbook*.

29. Where a natural person authorised to act on behalf of an *Appendix C business* is doing so in the course of employment with that business, it is acceptable for the firm not to identify and verify the identity of that person. However, the firm should verify the person's authority to act on behalf of the *Appendix C business*. One such example would be a director (or equivalent) of a *Bailiwick* fiduciary who is acting in the course of his fiduciary obligations or an administrator executing instructions on behalf of a CIS.

30. The firm is not obliged to deal with regulated *FSBs* or *PBs* in the jurisdictions listed in Appendix C as if they were local, notwithstanding that they meet the requirements identified in Appendix C. The firm may, in deciding whether or not to deal with a regulated *FSB* or *PB*, impose higher standards than the minimum standards identified in this *Handbook* where it considers this necessary.

31. The provisions in this Section cannot be applied to an *Appendix C business* (other than a trust and corporate service provider licensed by *the Commission*) which, acting as the trustee of a trust, is the *customer* or other *key principal* to a *business relationship* or *occasional transaction*.

9.6.1. Determination of Appendix C Countries and Territories

32. In accordance with Paragraphs 16(2) and 16A of *Schedule 3*, when exercising its functions *the Commission* must take into account information on, or in relation to:

    (a) the *ML*, *TF* and *PF risk* associated with particular countries, territories and geographic areas; and

(b) the level of cooperation it expects to receive from relevant authorities in those countries, territories and areas.

33. In making its determination of those jurisdictions listed in Appendix C, in addition to the factors set out in Paragraph 16(2) of *Schedule 3, the Commission* will also take into consideration several other factors including:

(a) the jurisdiction's membership of the FATF and/or a FATF-style regional body;
(b) reports and assessments by the FATF and/or other regional body for compliance with *the FATF Recommendations*;
(c) good governance indicators;
(d) the level of drug trafficking, bribery and corruption and other financial and organised crime within the jurisdiction;
(e) the extent of terrorism and terrorist financing activities within the jurisdiction; and
(f) the extent of proliferation financing activities within the jurisdiction.

34. When reviewing assessments undertaken by the FATF or other FATF-style regional bodies of a country/territory's compliance with *the FATF Recommendations*, particular attention is given to:

(a) the findings, recommendations and ratings of compliance with *the FATF Recommendations* (in particular Recommendations 10, 11,12 and 18); and
(b) the findings, recommendations and ratings of effectiveness of the country or territory's AML, CFT and CPF regime against the FATF's eleven 'Immediate Outcomes' set out within its methodology for compliance with *the FATF Recommendations*.

9.7. Receipt of Funds as Verification of Identity

35. Where the *customer* and *beneficial owner* have been identified and the *business relationship* or *occasional transaction* is considered to be low *risk*, the firm may consider the receipt of *funds* to provide satisfactory means of verifying identity.

36. In order to utilise this provision, the firm must ensure that:

(a) all initial and future *funds* are received from an *Appendix C business*;
(b) all initial and future *funds* come from an *account* in the sole or joint name of the *customer* or *beneficial owner*;
(c) payments are only paid to an *account* in the *customer's* name (i.e. no third party payments allowed), or in respect of real estate *transactions*, to an *account* in the name of the vendor of the property or in the name of the legal professional acting on behalf of the purchaser;
(d) no changes are made to the product or service that enable *funds* to be received from or paid to third parties; and
(e) no cash withdrawals are permitted other than by the *customer*, or a *beneficial owner*, on a face-to-face basis where the identity of the *customer* or *beneficial owner* can be confirmed, and in the case of significant cash transactions, the reasons for cash withdrawal are verified.

37. The firm must ensure that, once a *business relationship* has been established, should any of the conditions set out in *Commission Rule* 9.36. no longer be met, full verification of the identity of the *customer* and *beneficial owner* is carried out in accordance with the requirements of *Schedule 3* and this *Handbook*.

38. Should the firm have reason to suspect the motives behind a particular transaction or believe that the *business relationship* or *occasional transaction* is being structured to avoid the firm's standard *CDD* measures, it must ensure that the receipt of *funds* is not used to verify the identity of the *customer* or *beneficial owner*.

39. The firm must retain documentary evidence to demonstrate the reasonableness of its conclusion that the *risk* of the *business relationship* being established or the *occasional transaction* being undertaken is low.

9.8. Intermediary Relationships

40. An *intermediary relationship* is where the firm enters into a *business relationship* with an *intermediary* who is acting for or on behalf of its customers and where the *business relationship* the firm has is with the *intermediary* and not the *intermediary's* customers. If the firm has assessed the *ML, TF* and *PF risks* of the relationship with the *intermediary* as low, it may, subject to certain criteria being met and only in respect of certain qualifying products and services, treat the *intermediary* as its *customer* for *CDD* purposes, instead of identifying and verifying the identity of the *intermediary's* customer(s).

41. The firm should be aware that money launderers are attracted by the availability of complex products and services that operate internationally within a reputable and secure financial services environment. In this respect, the firm should be alert to the risk of an *intermediary relationship* being used to mask the true beneficial ownership of an underlying customer for criminal purposes.

42. Section 9.8.2. of this *Handbook* sets out the criteria which must be met for an *intermediary relationship* to be established by the firm. In such cases the firm will not have a direct relationship with the *intermediary's* customer and it will therefore not be necessary to apply *CDD* measures to the *intermediary's* customers, unless the firm considers this course of action to be appropriate in the circumstances. The *intermediary* does however have a direct relationship with its customer.

9.8.1. Risk Assessment

43. Before establishing an *intermediary relationship*, the firm must undertake a *relationship risk assessment* of the proposed *business relationship* with the *intermediary*.

44. Such an assessment will allow the firm to determine the *risk* in placing reliance on an *intermediary* and to consider whether it is appropriate to treat the *intermediary* as the firm's *customer* or whether it feels the *risk* would be better managed if it were to:

(a) treat the *intermediary* as an *introducer* in accordance with Chapter 10 of this *Handbook*; or
(b) apply *CDD* measures to the *customer* (including the *beneficial owner* and other *key principals*) for whom the *intermediary* is acting.

45. Chapter 10 of this *Handbook* provides for the identification and verification requirements in relation to introduced *business relationships*, i.e. where an *Appendix C business* enters into a *business relationship* with the firm on behalf of one or more third parties, who are its *customers*.

9.8.2. Criteria for Establishing an Intermediary Relationship

46. When establishing an *intermediary relationship*, the firm must apply *CDD* measures to the *intermediary* to ensure that the *intermediary* is either:

(a) an *Appendix C business*; or
(b) a wholly owned nominee subsidiary vehicle of an *Appendix C business* which applies the policies, procedures and controls of, and is subject to oversight from, the *Appendix C business*;

excluding a trust and corporate service provider unless that trust and corporate service provider is licensed under *the Fiduciary Law*.

47. Where the condition in *Commission Rule* 9.46. is met and the *business relationship* with the *intermediary* has been assessed as being low *risk*, the firm can exercise its own judgement in the circumstances as to the level of *CDD* measures to be applied to the *intermediary*. However, at a minimum the firm must:

    (a) identify and, subject to the provisions of Section 9.6. of this *Handbook*, verify the identity of the *intermediary*; and
    (b) receive written confirmation from the *intermediary* which:

        (i) confirms that the *intermediary* has appropriate *risk*-grading procedures in place to differentiate between the *CDD* requirements for *high risk relationships* and *low risk relationships*;
        (ii) contains adequate assurance that the *intermediary* applies appropriate and effective *CDD* measures in respect of its customers, including *ECDD* measures for *PEPs* and other *high risk relationships*;
        (iii) contains sufficient information to enable the firm to understand the purpose and intended nature of the *intermediary relationship*; and
        (iv) confirms that the *account* will only be operated by the *intermediary* and that the *intermediary* has ultimate, effective control over the relevant product or service.

48. Where an *intermediary relationship* has been established, the firm must prepare and retain documentary evidence of the following:

    (a) the adequacy of its process to determine the *risk* of the *intermediary relationship* and the reasonableness of its conclusions that it is a *low risk relationship*;
    (b) that it has applied *CDD* measures to the *intermediary*; and
    (c) that the *intermediary relationship* relates solely to the provision of products or services which meet the requirements of Section 9.8.3. below.

49. In circumstances where the criteria for an *intermediary relationship* are not completely satisfied or are no longer met (for example, because the proposed *intermediary* is not an *Appendix C business* or the *risk* of the *intermediary relationship* has been assessed as being other than low) then the relationship must not be considered as an *intermediary relationship*.

50. Where the firm has determined, in accordance with *Commission Rule* 9.49., that it cannot treat an *intermediary* as the *customer*, the firm must treat the underlying customers of the *intermediary* as if they were the firm's *customers* and must apply its own *CDD* measures in accordance with the requirements of *Schedule 3* and this *Handbook*.

51. The firm should always consider whether the *risk* would be better managed if it applied *CDD* measures to the person or *legal arrangement*, including the *beneficial owner* and other *key principals*, for whom the *intermediary* is acting rather than treating the *intermediary* as its *customer*.

52. The following are examples of steps the firm could take where, in accordance with *Commission Rule* 9.50., the firm is required to apply *CDD* measures to an *intermediary's* customers:

    (a) open individual *accounts* in the names of each of the *customers* on behalf of whom the *intermediary* was acting and apply *CDD* measures to each of those *customers*, including the *beneficial owners* and other *key principals*; or

(b) open an *account* in the name of the *intermediary*, provided that the firm also receives a complete list of the underlying *customers* from the *intermediary* to allow it to apply its own *CDD* measures to those *customers*, including the *beneficial owners* and other *key principals*.

9.8.3. Qualifying Products and Services

53. For an *intermediary* to be considered as the *customer* of the firm, the *intermediary relationship* must be for the provision of one of the following products and services:

(a) Investment of life company *funds* to back the life company's policyholder liabilities where the life company opens an *account* (see Section 9.8.3.1. below);
(b) Undertaking various restricted activities by a POI licensee, as part of its relationship falling within the scope of *the POI Law*, with another regulated *FSB* where the *funds* (and any income) may not be returned to a third party unless that third party was the source of *funds* (see Section 9.8.3.2. below);
(c) Investments into a CIS or NGCIS (for example, by a discretionary or advisory investment manager or custodian) acting in its own name and as the registered owner of the shares or units of the CIS (see Section 9.8.3.3. below); or
(d) The offering of insurance products to another regulated *FSB* by a Guernsey licensed insurer, as part of its relationship falling within the scope of *the IB Law*.

9.8.3.1. Investment of Life Company Funds

54. Where the firm is licensed under *the Banking Law* and provides services to a life insurance company through the opening of an *account* for the investment of *funds* to back the life company's policyholder liabilities, the firm can treat the life insurance company as its *customer*.

55. Where the firm is licensed under *the POI Law* and a life insurance company is investing its policy holder *funds* into a CIS authorised or registered by *the Commission* or an NGCIS, the firm can treat the life insurance company as its *customer*.

56. If the *account* or investment has a policy identifier then the firm must require an undertaking from the life company that it is the legal and beneficial owner of the *funds* and that the policyholder has not been led to believe that he or she has rights over an *account* or investment in *the Bailiwick*.

9.8.3.2. Investment Activity

57. Where the firm is licensed under *the POI Law* and undertakes various restricted activities within the scope of its licence as part of its relationship with another regulated *FSB*, the firm can treat that regulated *FSB* as its *customer*.

58. Where the firm utilises these provisions, any *funds* received from the *intermediary* (and any income resulting from the investment of such) must not be returned to a third party, unless that third party was the source of the *funds* and the firm is *satisfied* that the involvement of the third party does not pose an increased *ML, TF* or *PF risk*.

9.8.3.3. Investments into Collective Investment Schemes

59. Where the firm has been nominated in accordance with Paragraph 4.59. and an investment is made into a CIS or NGCIS (referred to in this section as a "CIS") by an *intermediary*, for example, a discretionary or advisory investment manager or custodian acting in its own name and as the registered owner of the shares as set out in Section 4.8.2. of this *Handbook*, the *nominated firm* can treat the *intermediary* as its *customer*.

60. Investments made into a CIS via an *intermediary* as described under *Commission Rule* 4.72.(b)-(c), where the identity of the underlying investors is not disclosed to the CIS or the *nominated firm*, is common practice within the fund sector across the world and is recognised within guidance issued by IOSCO, the Basel Committee on Banking Supervision and in the European Supervisory Authorities' ("ESAs") Risk Factors Guidelines issued under the Fourth Anti-Money Laundering Directive.

61. Notwithstanding the above, the ability for an underlying investor to invest into a CIS on an undisclosed basis increases the *risk* of a CIS being abused for *ML, TF* or *PF* purposes. This is particularly relevant where there are a very limited number of investors in a CIS who could exercise control over the assets of that CIS, either through ownership or by other means. In this respect it is possible for an individual person or family office to hold, via an *intermediary* or *intermediaries*, more than 25% of the shares/units or voting rights of a CIS, or exercise control through other means, which as identified under *the Bailiwick's* Beneficial Ownership regime, would classify the underlying investor as a *beneficial owner*, but their identity would not be known.

62. The *nominated firm* should be aware that certain types of CIS, such as hedge funds, real estate and private equity funds, tend to have a smaller number of investors which can be private individuals as well as institutional investors, for example, pension funds or funds of funds. CISs that are designated for a very limited number of high-net-worth individuals or family offices can have an inherently higher *risk* of abuse for *ML, TF* and/or *PF* purposes as compared to retail or institutional funds. In such cases, underlying investors are more likely to be in a position to exercise control over the CIS and use the CIS as a personal asset holding vehicle.

63. Personal asset holding vehicles should not be authorised/registered under *the POI Law*, as Paragraph 1(1)(b) of Schedule 1 to *the POI Law* states, inter alia:

> 'a CIS is any arrangement relating to property of any description (including money)…in which the investors do not have a day-to-day control over the management of the property to which the arrangement relates (whether or not they have any right to be consulted or give directions)'.

64. However, the *nominated firm* should be aware that an authorised or registered CIS could have, or may develop over time, the attributes of a personal asset holding vehicle.

65. Where the *nominated firm* wishes to utilise the *intermediary* provisions in respect of a CIS which is designated for a very limited number of investors, the *nominated firm* must have assessed the risk of the CIS being used by those investors as a personal asset holding vehicle as low. The conclusions of this assessment must be documented and reviewed on a periodic basis.

66. In conducting its assessment in accordance with *Commission Rule* 9.65. above, the *nominated firm* should consider factors such as the manner in which the shares or units of the CIS are distributed; the powers afforded to the share/unit holders of the CIS and their ability to influence any decision making; and details of any unusual connections between share/unit holders, board members and other parties connected with the CIS.

67. The assessment undertaken by the *nominated firm* could form part of its *relationship risk assessment* of the particular CIS, or be undertaken and recorded as a separate assessment.

68. Where the CIS targets institutional investors, as opposed to individuals, or retail investors through professional intermediaries, the risk of the CIS becoming a personal asset holding vehicle, for which a small group of individuals would be considered *beneficial owners* under *the Bailiwick's* Beneficial Ownership regime, is likely to be low.

69. Similarly, a CIS could be established by an *Appendix C business* as an in-house scheme for that *Appendix C business'* customers and for which the *Appendix C business* would be acting as the *intermediary* (i.e. the registered share/unit holder). Even in these cases, the *nominated firm* could, after reasonable enquiries about the CIS' distribution and operation, determine that the risk of that CIS being used as a personal asset holding vehicle is low.

70. Where the *nominated firm* has assessed that the risk of a CIS being used as a personal asset holding vehicle is other than low, it must not treat an *intermediary* as its *customer* and must look through the *intermediary relationship* to apply *CDD* measures (including *ECDD* and *enhanced measures* as applicable) to the *intermediary's* underlying customers, including the *beneficial owners* and other *key principals*.

9.8.3.4. Insurance Activity

71. Where the firm is licensed under *the IB Law* and offers insurance products within the scope of its licence as part of its relationship with another regulated *FSB*, the firm can treat that regulated *FSB* as its *customer*.

72. Where the firm utilises these provisions, any *funds* received from the *intermediary* (and any income resulting from the investment of such) must not be returned to a third party, unless that third party was the source of the *funds* and the firm is *satisfied* that the involvement of the third party does not pose an increased *ML, TF* or *PF risk*.

9.9. Pooled Bank Accounts

73. *Banks* often accept pooled deposits on behalf of *FSBs* and other professional firms. These *accounts* may contain the *funds* of more than one underlying customer and are generally held on an undisclosed basis.

74. Where the firm is licensed by *the Commission* under *the Banking Law* and has identified an *account* operated by it on behalf of one of the following types of *account* holder, the firm may treat this party as its *customer*:

(a) an *account* in the name of a fiduciary licensed by *the Commission*, or supervised by an equivalent authority in the Bailiwick of Jersey, or a wholly owned subsidiary of such a business which meets the requirements of Paragraph 9.75. below, where:

(i) the holding of *funds* in the *account* is on a short-term basis; or
(ii) the holding of *funds* in the *account* relates to the provision of treasury/cash management services by the fiduciary on behalf of its customers;

(b) an *account* in the name of a firm of lawyers or estate agents registered with *the Commission*, or supervised by an equivalent authority in the Bailiwick of Jersey, where the holding of *funds* in the *account* is on a short-term basis and is necessary to facilitate a transaction;

(c) a client money *account* in the name of a firm licensed under *the POI Law*, or subject to equivalent licensing and oversight by an authority in the Bailiwick of Jersey, or a wholly owned subsidiary of such a licensed business, which is providing services to its parent to enable it to fulfil activities for which it is licensed, such as custody & settlement, where the *funds* are subject to the Licensees (Conduct of Business) Rules and Guidance, 2021 or equivalent legislation in the Bailiwick of Jersey;

(d) a client money *account* in the name of a firm licensed under *the IMII Law*, or subject to equivalent licensing and oversight by an authority in the Bailiwick of Jersey, where the

funds are subject to the Insurance Intermediaries Rules and Guidance, 2021 or equivalent legislation in the Bailiwick of Jersey;

(e) a client money *account* in the name of a firm licensed under the *LCF Law*, or subject to equivalent licensing and oversight by an authority in the Bailiwick of Jersey, where the *funds* are subject to the Lending, Credit and Finance Rules and Guidance, 2023, or equivalent legislation in the Bailiwick of Jersey; or

(f) a client money account for businesses with an established place of business in the Bailiwick operating outside of the financial and prescribed business sectors, to facilitate its non-financial services business, such as Bailiwick- based property management, auction sales and payroll, where the funds are derived from an account held with a financial institution which is supervised for AML/CFT/CPF purposes i.e. the receipt of physical cash would not be permitted.

75. The requirements referred to in Paragraph 9.74.(a) and (c) above are that the wholly owned subsidiary:

(a) has no customers which are not customers of the fiduciary or the POI licensee in *the Bailiwick* or of an equivalent licensed business in the Bailiwick of Jersey; and

(b) applies the same AML, CFT and CPF policies, procedures and controls as the fiduciary or the POI licensee in *the Bailiwick* or of an equivalent licensed businesses in the Bailiwick of Jersey.

76. For the purposes of Paragraphs 9.74.(a)(i) and (b) above, *funds* are considered to have been held on a 'short-term' basis where they are held, undisclosed, for no longer than 40 days.

77. Where the firm is licensed by *the Commission* under *the Banking Law* and holds deposits on a fiduciary basis on behalf of an overseas *bank* falling within the definition of an *Appendix C business*, the firm should treat the overseas *bank* as its *customer* in accordance with Section 9.6. of this *Handbook*.

9.9.1. Establishing a Pooled Banking Relationship

78. Where the firm operates an *account* falling within the provisions of Paragraph 9.74. and the *business relationship* with the *account* holder has been assessed as being low *risk*, the firm can exercise its own judgement as to the level of *CDD* measures to be applied to the *account* holder in the particular circumstances. However, as a minimum the firm must:

(a) identify and, subject to the provisions of Section 9.6. of this *Handbook*, verify the identity of the *account* holder; and

(b) receive written confirmation from the *account* holder which:

(i) confirms that the *account* holder has appropriate *risk*-grading procedures in place to differentiate between the *CDD* measures appropriate for *high risk relationships* and those for *low risk relationships* where the account holder falls within Paragraph 9.74 (a) – (e) above;

(ii) contains adequate assurance that the *account* holder applies appropriate and effective *CDD* measures in respect of its customers (and the *beneficial owners* and other *key principals*), including *ECDD* measures for *PEPs* and other *high risk relationships* where the account holder falls within Paragraph 9.74 (a) – (e) above;

(iii) contains sufficient information to enable the firm to understand the purpose and intended nature of the relationship;

(iv) confirms that the *account* will only be operated by the *account* holder and that the *account* holder has ultimate effective control over the relevant product or service; and

(v) where the *account* is operated by a business falling within 9.74(f), written confirmation from the *account* holder that the account will be used for no other purpose than to facilitate its business activity.

79. Where a *business relationship* has been established with an *account* holder for the provision of a pooled *account*, the firm must prepare and retain documentary evidence of the following:

(a) the adequacy of its processes to determine the *risk* of the *business relationship* with the *account* holder and the reasonableness of its conclusions that it is a *low risk relationship*;
(b) that it has applied *CDD* measures in respect of the *account* holder; and
(c) that the *business relationship* with the *account* holder relates solely to the provision of an *account* falling within Paragraph 9.74.(a)-(f) above.

80. Where the firm operates a pooled *account* on behalf of an *account* holder which:

(a) does not fall within Paragraph 9.74.(a)-(f) above; or
(b) has been assessed as being other than low *risk*, for example, because the firm has concerns in respect of the manner in which a pooled *account* is being operated,

then the firm must not treat the *account* holder as its *customer* and must apply its own *CDD* measures on the underlying *customers* (including the *beneficial owners* and other *key principals*) within the pooled *account* in accordance with the requirements of *Schedule 3* and this *Handbook*.

81. The firm should always consider whether the *risk* would be better managed if the firm applied *CDD* measures on the *customer*, *beneficial owner* and other *key principals* for whom the *account* holder is acting rather than treating the *account* holder as the *customer*.

Chapter 10
Introduced Business

Contents of this Chapter

10.1. Introduction

1. An introduced *business relationship* or *occasional transaction* is a formal arrangement whereby an *Appendix C business* (or an overseas branch of, or member of the same group of bodies as, the firm) acting on behalf of one or more third parties who are also its customers, establishes a *business relationship* or undertakes an *occasional transaction* with a *specified business* on behalf of that customer. Introduced *business relationships* or *occasional transactions* may be on behalf of a single *customer* or on behalf of more than one *customer*, including a pool of such persons.

2. A *business relationship* established by an *introducer* on behalf of more than one of its *customers* is described by this *Handbook* as a pooled relationship. Further information on pooled relationships can be found in Section 9.9. of this *Handbook*.

3. This Chapter does not apply to outsourcing or agency relationships. Under an *introducer* arrangement the third party will apply its own procedures to perform the *CDD* measures for the *customer*, subject to an initial assessment of the third party by the firm and to ongoing periodic testing. This contrasts with an outsourced or agency relationship, where the outsourced service provider or agency is regarded as part of the delegating firm, applying the delegating firm's *CDD* measures in accordance with the delegating firm's procedures and subject to oversight and control of the effective implementation of those procedures by the delegating firm.

10.2. Risk Exposure

4. Introduced business by its very nature has the capacity to be high *risk*, i.e. relying on a third party to have adequately applied *CDD* measures to mitigate the *risk* of the firm being involved in, or abused for, *ML* or *TF*. In this respect, while the firm is still required to hold sufficient identifying information about its *customer* and the *beneficial owner* thereof, the firm places reliance on a third party to have adequately and appropriately verified the identity of that *customer* and *beneficial owner*, and to retain evidence of that verification.

5. The firm must recognise the increased *risk* posed by introduced business and ensure that its consideration of these *risks* is adequately documented within its *business risk assessments*.

6. In addition to an explanation of any *risks* identified, the firm's *business risk assessments* should also include a description of the policies, procedures and controls established to mitigate and manage such *risk*.

7. The firm must consider, for each *business relationship* or *occasional transaction*, whether it is appropriate on the basis of *risk* to rely on a certificate or summary sheet from an *introducer* in accordance with Paragraph 10 of *Schedule 3* or whether it considers it necessary to do more.

8. In accordance with Paragraph 10(3) of *Schedule 3*, where reliance is placed upon an *introducer*, the responsibility for complying with the relevant provisions of Paragraph 4 of *Schedule 3* shall remain with the firm.

10.3. Establishing an Introducer Relationship

9. In accordance with Paragraph 10(1) of *Schedule 3*, in the circumstances set out in Paragraph 10(2) as reflected below, the firm may accept a written confirmation of identity and other matters from an *introducer* in relation to the requirements of Paragraph 4(3)(a)–(e) of *Schedule 3*, provided that:

   (a) the firm also requires copies of *identification data* and any other relevant *documentation* on the identity of the *customer* and *beneficial owner* to be made available by the *introducer* to the firm immediately upon request; and

(b) the *introducer* keeps such *identification data* and *documents*.

10. In accordance with Paragraph 10(2) of *Schedule 3*, the circumstances referred to in Paragraph 10.9. above are that the *introducer*:

(a) is an *Appendix C business*; or
(b) is either an overseas branch office of, or a member of the same group of *legal persons* or *legal arrangements* as, the firm, and

(i) the ultimate *legal person* or *legal arrangement* of the group of *legal persons* or *legal arrangements* of which both the *introducer* and the firm are members, is an *Appendix C business*; and
(ii) the conduct of the *introducer* is subject to requirements to forestall, prevent and detect *ML* and *TF* (including the application of any appropriate additional measures to effectively handle the *risk* of *ML* or *TF*) that are consistent with those in *the FATF Recommendations* in respect of such a business (particularly Recommendations 10, 11 and 12), and the *introducer* has implemented a programme to combat *ML* and *TF* that is consistent with the requirements of Recommendation 18; and
(iii) the conduct both of the *introducer*, and of the group of *legal persons* or *legal arrangements* of which both the *introducer* and the firm are members, is supervised or monitored for compliance with the requirements referred to in (ii) above, by *the Commission* or an overseas regulatory authority.

11. In addition to the confirmations required by Paragraph 10(1) of *Schedule 3*, when establishing an *introducer* relationship, the firm must also *satisfy* itself that the *introducer*:

(a) has appropriate *risk*-grading procedures in place to differentiate between the *CDD* requirements for *high risk relationships* and *low risk relationships*;
(b) applies appropriate and effective *CDD* measures to its *customers*, and the *beneficial owners* and other *key principals* thereof, including *ECDD* measures to *foreign PEPs* and other *high risk relationships*; and
(c) has appropriate record keeping requirements similar to those set out in Paragraph 14 of *Schedule 3*.

12. The *CDD* measures referred to in Paragraph 10(1) of *Schedule 3* include the following elements:

(a) identifying the *customer* and verifying the *customer's* identity using *identification data*;
(b) identifying any person purporting to act on behalf of the *customer* and verifying that person's identity and their authority to so act;
(c) identifying the *beneficial owner* and taking reasonable measures to verify the identity of the *beneficial owner*, including, in the case of a *customer* which is a *legal person* or *legal arrangement*, taking measures to understand the nature of the *customer*'s business and its ownership and control structure;
(d) determining whether the *customer* is acting on behalf of another person and, if the *customer* is so acting, taking reasonable measures to identify that other person and to obtain sufficient *identification data* to verify the identity of that other person; and
(e) understanding, and as appropriate obtaining information to support this understanding of, the purpose and intended nature of the *business relationship* or *occasional transaction*.

13. A template certificate which may be used by the firm for introduced business can be found in Appendix F to this *Handbook*.

14. The firm must take appropriate steps to be *satisfied* that the *introducer* will supply, immediately upon request, certified copies or originals of the *identification data* and other relevant *documents*

it has collected under the *CDD* measures applied to its *customers*, including the *beneficial owner* and other *key principals* thereof.

15. Where an introduced *business relationship* presents a high *risk* of *ML, TF* or *PF*, consideration should be given to whether it is appropriate for the firm to rely solely upon the information provided by the *introducer* or whether supplemental *CDD* information and/or *documentation* is required.

16. It is the responsibility of the *introducer* to inform the firm of any changes to the parties involved in an *introducer* arrangement, for example, to the relationship structure, the profile, or any *CDD* held. As part of establishing an introduced relationship the firm should seek confirmation from the *introducer* that it will notify the firm of changes to the *customer*, or the *beneficial owner* thereof, without delay.

10.4. Testing

17. The firm must have a scheduled programme of testing to ensure that, on an on-going basis, an *introducer* is able to fulfil the requirement that certified copy or original *identification data* that it has collected will be provided to the firm immediately upon request. This will involve the firm adopting ongoing procedures to ensure it has the means to obtain that *identification data*.

18. The testing programme should be *risk*-based and commensurate with the *risk* exposure, size and scope of the business introduced. The programme should provide appropriate and sufficient assurance to the firm that it can continue to rely upon an *introducer* to fulfil its obligation to provide *identification data* immediately upon request. In this respect, priority should be given to those *introducers* posing the highest *risk* to the firm, i.e. those with the greatest number of introduced relationships and/or the highest *risk customers*.

19. Notwithstanding the above, the firm should set a minimum timeframe within which all *introducers* will be subject to appropriate periodic testing and record this within its *introducer* testing procedure.

20. The scope of the testing undertaken should include verification that the information received from the *introducer* on a certificate or summary sheet containing information about the identity of the underlying *customer*, *beneficial owner* and other *key principals*, continues to be accurate and up to date. This allows the firm to determine whether, based on any changes, it wishes to continue to rely upon the arrangement or whether the firm may wish to seek further information from the *introducer* about the underlying *customer* and/or associated *key principals*.

21. Where, as a result of a test carried out, the firm is not *satisfied* that the *introducer* has appropriate policies and procedures in place, maintains appropriate records, or will provide evidence of those records immediately if requested to do so, the firm must apply *CDD* measures in accordance with Paragraph 4 of *Schedule 3* for that *customer*, including the *beneficial owner* and other *key principals* thereof, and give consideration to terminating its relationship with the *introducer*.

10.5. Termination

22. In the event that an *introducer* terminates its relationship with an introduced *customer*, the firm should consider how best it will continue to maintain compliance with its *CDD* obligations for that *customer* and associated *key principals*. In this respect, the firm should give consideration to the following:

    (a) instructing the *introducer* to provide the firm with copies of the *identification data* held for the *customer*, *beneficial owner* and other *key principals*; or

(b) gathering its own *identification data* on the *customer*, *beneficial owner* and other *key principals*, and terminating the *introducer* relationship.

10.6. Group Introducers

23. Where a *customer* is introduced to the firm by a member of the firm's wider group, it is not necessary for the identity of the *customer* or any *key principal* to be re-verified, provided that the group entity acting as *introducer* provides the firm, in accordance with Paragraph 10(1) of *Schedule 3*, with written confirmation that it:

(a) applies *CDD* requirements in line with Paragraph 4 of *Schedule 3*;
(b) meets the requirements of Paragraph 10(2) of *Schedule 3* to be classified as an *introducer*;
(c) applies record keeping requirements in line with Paragraph 14 of *Schedule 3*; and
(d) will provide copies of *identification data* immediately upon request.

24. Where the firm has access to the *identification data* of the introducing group member's *customers* and associated *key principals*, for example, via a group-wide *document* management system, the testing obligations set out in *Commission Rule* 10.17. will be deemed to have been met, provided the firm reviews the *identification data* held on a periodic basis.

25. Notwithstanding the above, the firm must not regard group introduced business as intrinsically low *risk* and must decide, on the basis of *risk*, whether it is appropriate to rely on a certificate or summary sheet from a group *introducer*. Where a certificate or summary sheet is not deemed appropriate, the firm must consider the steps it is required to take, bearing in mind that the ultimate responsibility for the application of *CDD* measures remains with the firm.

10.7. Chains of Introducers

26. Chains of *introducers* are not permitted and the firm must not place reliance on an *introducer* which forms part of a chain.

27. This requirement is intended to avoid a situation whereby, should the middle institution fall away, the receiving business is left in difficulty vis-à-vis obtaining copies of *identification data* and other relevant *documentation* relating to the introduced *customer* from the original *introducer*.

Chapter 11
Monitoring Transactions and Activity

Contents of this Chapter

11.1. Introduction

1. The regular monitoring of a *business relationship*, including any transactions and other activity carried out as part of that relationship, is one of the most important aspects of effective ongoing *CDD* measures.

2. It is vital that the firm understands a *customer's* background and is aware of changes in the circumstances of the *customer* and *beneficial owner* throughout the life-cycle of a *business relationship*. The firm can usually only determine when it might have reasonable grounds for knowing or suspecting that *ML, TF* and/or *PF* is occurring if it has the means of assessing when a transaction or activity falls outside the normal expectations for a particular *business relationship*.

3. There are two strands to effective ongoing monitoring:

   (a) The first relates to the transactions and activity which occur on a day-to-day basis within a *business relationship* and which need to be monitored to ensure they remain consistent with the firm's understanding of the *customer* and the product or service it is providing to the *customer*.
   (b) The second relates to the *customer* themselves and the requirement for the firm to ensure that it continues to have a good understanding of its *customers* and their *beneficial owners*. This is achieved through maintaining relevant and appropriate *CDD* and applying appropriate ongoing screening.

4. This Chapter deals with the requirement for the firm to monitor *business relationships* on an ongoing basis, including the application of scrutiny to large and unusual or complex transactions or activity so that *ML, TF* and *PF* may be identified and prevented.

11.2. Objectives

5. A key prerequisite to managing the *risk* of a *business relationship* is understanding the *customer*, and *beneficial owner*, and where changes to those parties occur. It is also important to maintain a thorough understanding of the *business relationship* and to appropriately monitor transactions in order to be in a position to detect, and subsequently report, suspicious activity.

6. The type of monitoring applied by the firm will depend on a number of factors and should be developed with reference to the firm's *business risk assessments* and *risk appetite*. The factors forming part of this consideration will include the size and nature of the firm's business, including the characteristics of its *customer*-base and the complexity and volume of expected transactions or activity.

7. The monitoring of *business relationships* should involve the application of scrutiny to large and unusual or complex transactions, as well as to patterns of transactions or activity, to ensure that such transactions and activity are consistent with the firm's knowledge of the *customer*, their business and *risk* profile, including where necessary, the source of *funds*. Particular attention should be paid to *high risk relationships* (for example, those involving *foreign PEPs*), high *risk* countries and territories and high *risk* transactions.

8. An unusual transaction or activity may be in a form that is inconsistent with the expected pattern of activity within a particular *business relationship*, or with the normal business activities for the type of product or service that is being delivered. For example, unusual patterns of transactions with no apparent or visible economic or lawful purpose.

9. The nature of the monitoring in any given case will depend on the business of the firm, the frequency of activity and the types of business. Monitoring may include reference to: specific types of transactions; the relationship profile; a comparison of activities or profiles with that of a similar *customer* or peer group; or a combination of these approaches.

11.3. Obligations

10. In accordance with Paragraph 11(1) of *Schedule 3*, the firm shall perform ongoing and effective monitoring of any *business relationship*, which shall include –

    (a) reviewing *identification data* and records to ensure they are kept up to date, accurate and relevant, and updating such data and records when they are not up to date, accurate or relevant;
    (b) scrutinising any transactions or other activity to ensure that the transactions are consistent with the firm's knowledge of the *customer*, their business and *risk* profile (including, where necessary, the source of *funds*) and paying particular attention to all –

        (i) complex transactions;
        (ii) transactions which are both large and unusual; and
        (iii) unusual patterns of activity or transactions,

        which have no apparent economic purpose or no apparent lawful purpose; and
    (c) ensuring that the way in which *identification data* is recorded and stored is such as to facilitate the ongoing monitoring of each *business relationship*.

11. In accordance with Paragraph 11(2) of *Schedule 3*, the extent of any monitoring carried out and the frequency at which it is carried out shall be determined on the basis of materiality and *risk* including, without limitation, whether or not the *business relationship* is a *high risk relationship*.

12. Examples of the additional monitoring arrangements for *high risk relationships* could include:

    (a) undertaking more frequent reviews of *high risk relationships* and updating *CDD information* on a more regular basis;
    (b) undertaking more regular reviews of transactions and activity against the profile and expected activity of the *business relationship*;
    (c) applying lower monetary thresholds for the monitoring of transactions and activity;
    (d) reviews being conducted by persons not directly involved in managing the relationship, for example, the *MLCO*;
    (e) ensuring that the firm has adequate MI systems to provide the *board* and *MLCO* with the timely information needed to identify, analyse and effectively monitor *high risk relationships* and *accounts*;
    (f) appropriate approval procedures for high value transactions in respect of *high risk relationships*; and/or
    (g) a greater understanding of the personal circumstances of *high risk relationships*, including an awareness of sources of third party information.

13. The firm must consider the possibility for *legal persons* and *legal arrangements* to be used as vehicles for *ML*, *TF* and *PF*.

11.4. PEP Relationships

14. The system of monitoring used by the firm must provide for the ability to identify where a *customer* or *beneficial owner* becomes a *PEP* during the course of the *business relationship* and whether that person is a *foreign PEP*, *domestic PEP* or *international organisation PEP*.

15. In accordance with Paragraph 5(3)(a)(ii) of *Schedule 3*, where a *customer* or *beneficial owner* becomes a *foreign PEP* during the course of an existing *business relationship* or a *domestic PEP* or *international PEP* during the course of an existing high risk *business relationship*, as part of the *ECDD* measures subsequently applied the firm shall obtain senior management approval to continue that relationship.

16. Where the firm identifies during the course of a *business relationship* that the *customer* or *beneficial owner* is a *domestic PEP* or *international organisation PEP*, it should refer to the requirements of *Commission Rule* 8.45.

17. It is not expected that the firm will have a thorough knowledge of, or fully research, a family connection. The extent to which a connection is researched should be based upon the size, scale, complexity and involvement of the person in the context of the *business relationship* and the profile of the *business relationship*, including its asset value.

18. It is possible that family members and/or associates may not inform the firm, or even be aware, of their *PEP* status and therefore independent screening and monitoring should be conducted. It is also possible that an individual's *PEP* status may not be present at take-on, for example, where that person takes office during the life of a *business relationship*. It is therefore important that ongoing monitoring exists in order to identify changes of status and *risk* classification.

11.5. High Risk Transactions or Activity

19. When conducting ongoing monitoring, the following are examples of red flags which may indicate high *risk* transactions or activity within a *business relationship*:

(a) an unusual transaction in the context of the firm's understanding of the *business relationship* (for example, abnormal size or frequency for that *customer* or peer group, or a transaction or activity involving an unknown third party);
(b) funds originating from, or destined for, an unusual location, whether specific to an individual *business relationship*, or for a generic *customer* or product type;
(c) the unexpected dormancy of an *account*, or transactions or activity unexpectedly occurring after a period of dormancy;
(d) unusual patterns of transactions or activity which have no apparent economic or lawful purpose;
(e) an instruction to effect payments for advisory or consulting activities with no apparent connection to the known activities of the *customer* or their business;
(f) the involvement of charitable or political donations or sponsorship;
(g) a *relevant connection* with a country or territory that has significant levels of corruption, or provides funding or support for terrorist activities; or
(h) a *relevant connection* with a country or territory subject to targeted financial sanctions relating to *TF* or to *PF*.

20. Transactions or activity to or from jurisdictions specified in Appendix H to this *Handbook*, any *Commission* Notices, Instructions or Warnings and those covered by sanctions legislation applicable in *the Bailiwick* must be subject to a greater level of caution and scrutiny.

https://www.gfsc.gg/commission/financial-crime/notices-instructions-warnings

11.6. Real-Time and Post-Event Transaction Monitoring

21. Monitoring procedures should involve a combination of real-time and post-event monitoring. Real-time monitoring focuses on transactions and activity where information or instructions are

received before or as the instruction is processed. Post-event monitoring involves periodic, for example monthly, reviews of transactions and activity which have occurred over the preceding period.

22. Real-time monitoring of activity can be effective at reducing exposure to *ML*, *TF* and *PF* and predicate offences such as bribery and corruption, whereas post-event monitoring may be more effective at identifying patterns of unusual transactions or activities.

23. In this respect, regardless of the split of real-time and post-event monitoring, the over-arching purpose of the monitoring process employed should be to ensure that unusual transactions and activity are identified and flagged for further examination.

11.7. Automated and Manual Monitoring

24. The firm's monitoring processes should be appropriate having regard to its size, activities and complexity, together with the *risks* identified by the firm within its *business risk assessments*. While bigger firms with large volumes of transactions will likely favour an automated system, the firm may conclude that a manual real-time and/or post-event monitoring process is sufficient given the size and scale of its business.

25. Notwithstanding the method of monitoring used, in accordance with the requirements of Paragraph 11(2) of *Schedule 3*, the firm should adapt the parameters of its processes, in particular the extent and frequency of monitoring, on the basis of materiality and *risk*, including, without limitation, whether or not a *business relationship* is a *high risk relationship*.

26. In establishing the expected norms of a *business relationship* and in turn the appropriate parameters for its monitoring processes to be effective, the firm should consider, as a minimum, the nature and level of expected transactions and activity and the assessed *risk* of the *business relationships* that are being monitored.

27. The rationale for deciding upon either a manual or automated method of monitoring, together with the criteria in defining the parameters of that monitoring, should be based on the conclusions of the firm's *business risk assessments* and *risk appetite*. The decision made by the firm should be documented as part of this process, together with an explanation demonstrating why the *board* consider the chosen method to be appropriate and effective.

11.7.1. Automated Monitoring Methods

28. Where the firm has a large number of *business relationships* or a high level of activity, effective monitoring is likely to necessitate the automation of the monitoring process. Such automated systems may be used to facilitate the monitoring of significant volumes of transactions or *business relationships*, and associated *customers* and *beneficial owners*. Automated systems may also be utilised where the firm operates in an environment where the opportunity for human scrutiny of individual transactions and activity is limited, for example, in e-commerce.

29. The use of automated monitoring methods can be effective in both strands of ongoing monitoring:

    (a) identifying a transaction and/or activity which warrant further scrutiny; and
    (b) screening *customers* and *beneficial owners* to *business relationships*, as well as the *payers* and *payees* to individual transactions, for connections to persons subject to UN, UK or other sanction or posing an increased *risk*. For example, *PEPs*, those convicted of criminal acts, or those persons in respect of whom adverse media exists.

30. With regard to the monitoring of transactions and activity, exception procedures and reports can provide a simple but effective means of monitoring all incoming and outgoing transactions and activity to identify those involving, amongst other things:

(a) particular countries, territories or geographical locations;
(b) particular products, services and/or *accounts*; or
(c) transactions or activity falling outside of predetermined parameters within a given time frame.

31. Where an automated monitoring method is used, whether specific to the firm or a group-wide system, the firm must:

(a) understand how the system works and how to use the system (for example, making full use of guidance);
(b) understand when changes are to be made to the system (including the nature and extent of any changes);
(c) understand the system's coverage (including the extent of the transactions, activity and/or parties monitored);
(d) understand the sources of data used (including both the source(s) of internal data fed into the system and the source(s) of external data to which it is compared);
(e) understand the nature of the system's output (exceptions, alerts etc.);
(f) set clear procedures for dealing with potential matches, driven on the basis of *risk* rather than resources; and
(g) record the basis for discounting alerts (for example, false positives) to ensure there is an appropriate audit trail.

32. Subject to *Commission Rule* 11.33. below, the firm must ensure that the parameters of any automated system allow for the generation of alerts for large and unusual, complex, or higher *risk* transactions or activity which must be subject to further investigation.

33. Where the firm is a branch office or subsidiary of an international group and uses group-wide systems for transaction and activity monitoring, the ability for the firm to dictate the particular characteristics of the monitoring conducted by the system may be limited. Where this is the case, notwithstanding the group-wide nature of the system, the firm must be *satisfied* that it provides adequate mitigation of the *risks* applicable to the business of the firm.

34. The firm should be aware that the use of computerised monitoring systems does not remove the requirement for *relevant employees* to remain vigilant. It is essential that the firm continues to attach importance to human alertness. Factors such as a person's intuition; direct contact with a *customer* either face-to-face or on the telephone; and the ability, through practical experience, to recognise transactions and activities which do not seem to have a lawful or economic purpose, or make sense for a particular *customer*, cannot be automated.

11.8. Examination

35. In accordance with Paragraph 11(3) of *Schedule 3*, where within an existing *business relationship* there are complex, or large and unusual, transactions, or unusual patterns of transactions, which have no apparent economic or lawful purpose, the firm shall:

(a) examine the background and purpose of those transactions, and
(b) increase the degree and nature of monitoring of the *business relationship*.

36. As part of its examination, the firm should give consideration to the following:

(a) reviewing the identified transaction or activity in conjunction with the *relationship risk assessment* and the *CDD information* held;
(b) understanding the background of the activity and making further enquiries to obtain any additional information required to enable a determination to be made by the firm as to whether the transaction or activity has a rational explanation and economic purpose;
(c) reviewing the appropriateness of the *relationship risk assessment* in light of the unusual *transaction* or activity, together with any supplemental *CDD information* obtained; and
(d) considering the transaction or activity in the context of any other connected *business relationships* and the cumulative effect this may have on the *risk* attributed to those relationships.

37. For the purposes of Paragraph 11(3) of *Schedule 3*, what constitutes a large and unusual or complex transaction will be based on the particular circumstances of a *business relationship* and will therefore vary from *customer* to *customer*.

38. The firm must ensure that the examination of any large and unusual, complex, or otherwise higher *risk* transaction or pattern of transactions or other activity is sufficiently documented and that such *documentation* is retained in a readily accessible manner in order to assist *the Commission*, the *FIU*, other domestic competent authorities and auditors.

39. The firm must ensure that procedures are *maintained* which require that an internal disclosure is filed with the *MLRO* in accordance with the requirements of Chapter 13 of this *Handbook* where the circumstances of the transaction or activity raise a suspicion of *ML, TF* and/or *PF*.

40. Following the conclusion of its examination, the firm should give consideration to whether follow-up action is necessary in light of the identified transaction or activity. This could include, but is not limited to:

(a) applying *ECDD* measures where this is considered necessary or where the firm has re-assessed the *business relationship* as being high *risk* as a consequence of the transaction or activity;
(b) considering whether further *employee* training in the identification of large and unusual, complex, or higher risk transactions and activity is needed;
(c) subject to *Commission Rule* 11.33. above, considering whether there is a need to adjust the monitoring system (for example, refining monitoring parameters or enhancing controls for more vulnerable products, services and/or business units); and/or
(d) applying increased levels of on-going monitoring for particular relationships.

11.9. Ongoing Customer Due Diligence

41. The requirement to conduct ongoing *CDD* will ensure that the firm is aware of any changes in the development of a *business relationship*. The extent of the firm's ongoing *CDD* measures must be determined on a *risk*-sensitive basis. However, the firm must be aware that as a *business relationship* develops, the risks of *ML, TF* and *PF* may change.

42. *The Commission* would expect ongoing *CDD* to be conducted on a periodic basis in line with the requirement to review *relationship risk assessments* in accordance with Paragraph 3(4)(b) of *Schedule 3*, or where a trigger event occurs in the intervening period.

43. It should be noted that it is not necessary to re-verify or obtain current *identification data* unless an assessment has been made that the *identification data* held is not adequate for the assessed *risk* of the *business relationship* or there are doubts about the veracity of the information already held. Examples of such could include a material change in the way that the business of the *customer* is conducted which is inconsistent with its existing business profile, or where the firm

becomes aware of changes to a *customer's* or *beneficial owner's* circumstances, such as a change of address.

44. In order to reduce the burden on *customers* and other *key principals* in *low risk relationships*, trigger events (for example, the opening of a new *account* or the purchase of a further product) may present a convenient opportunity to review the *CDD information* held.

11.10. Oversight of Monitoring Controls

45. The *MLCO* should have access to, and familiarise his or her self with, the results and output from the firm's monitoring processes. Such output should be reviewed by the *MLCO* who in turn should report regularly to the *board*, providing relevant MI such as statistics and key performance indicators, together with details of any trends and actions taken where concerns or discrepancies have been identified.

46. The *board* should consider the appropriateness and effectiveness of the firm's monitoring processes as part of its annual review of the firm's *business risk assessments* and associated policies, procedures and controls. This should include consideration of the extent and frequency of such monitoring, based on materiality and *risk* as set out in the *business risk assessments*.

47. Where the firm identifies weaknesses within its monitoring arrangements, it should ensure that these are rectified in a timely manner and consideration should be given to *notifying the Commission* in accordance with the requirements of Section 2.7. of this *Handbook*.

Chapter 12
UN, UK and Bailiwick Sanctions

Contents of this Chapter

12.1. Introduction

1. Sanctions are imposed by the UN to further its aims of maintaining international peace and security. It imposes targeted financial sanctions and requires member states to implement them through Resolutions passed by the UN Security Council ("UNSCRs"). There are a range of UNSCRs relating to the prevention and suppression of terrorism and *terrorist financing* and the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These UNSCRs have effect in UK legislation via regulations made under the Sanctions and Anti-Money Laundering Act 2018 (the "Sanctions Act") which have automatic effect in the Bailiwick.

2. In addition to UNSCRs, the UK puts in place sanctions measures to fulfil foreign policy and defence objectives. The sanctions imposed on Russia and related interests as a result of the invasion of Ukraine are a prime example of the UK imposing sanctions to fulfil foreign policy and defence objectives.

3. Sanctions are imposed by the UN and/or the UK to apply restrictive measures against a country, regime, individual, entity, industry or type of activity believed to be violating international law and could include one or more of the following:

   (a) the freezing of *funds*;
   (b) the withdrawal of financial services;
   (c) a ban or restriction on trade;
   (d) a ban or restriction on travel; or
   (e) suspension from international organisations.

4. The ultimate objective of a sanction varies according to the situation. For instance, an arms embargo and a ban on the export of certain items or raw materials could be aimed at supporting a peace process and restricting the financing of weapons by combatants. Sanctions may also be aimed at preventing the proliferation of weapons of mass destruction, disrupting terrorist operations, or trying to change the policies and actions of the target. Sanctions of this kind are a tool used increasingly for enforcing foreign policy by putting pressure on a state or entity in order to maintain or restore international peace and security. Often, sanctions are used as an alternative to force.

5. This Chapter outlines the statutory provisions applicable to firms within *the Bailiwick* concerning UN, UK *and Bailiwick* sanctions. It also covers the policies, procedures and controls required in order to comply with *the Bailiwick's* sanctions regime and the provisions for the disclosure of information to the relevant authorities in respect of designated persons and the freezing of *funds*.

12.2. The Bailiwick's Sanctions Regime

6. The *Bailiwick* implements UNSCR 1373 (2001) in respect of *TF* in two ways. The first is under the Sanctions (Implementation of UK Regimes) (Bailiwick of Guernsey) (Brexit) Regulations, 2020 ("the 2020 regulations"). The 2020 regulations implement both the Counter-Terrorism (Sanctions) (EU Exit) Regulations 2019 and the Counter-Terrorism (International Sanctions) (EU Exit) Regulations 2019 in *the Bailiwick*. All persons designated under these UK regulations are included in the regime.

7. The second way in which *the Bailiwick* implements UNSCR 1373 (2001) is under the Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011 ("*Terrorist Asset Freezing Law*"), which imposes financial sanctions on persons designated by the States of Guernsey Policy & Resources Committee. These sanctions effectively mirror the financial sanctions under the UK regulations. They are subject to exemptions applicable to certain transactions or activities, and also do not

apply to anything that is permitted under a licence granted by the States of Guernsey Policy & Resources Committee.

8. In order to exercise its powers of designation, the States of Guernsey Policy & Resources Committee must first reasonably suspect that the potential designation target is:

   (a) involved in terrorist activity;
   (b) owned or controlled directly or indirectly by a person involved in terrorist activity; or
   (c) acting on behalf of, or at the direction of, a person involved in terrorist activity.

9. There are three sanctions regimes in force in *the Bailiwick* that specifically concern proliferation and *proliferation financing* activities. These are the regimes imposed by the UN and UK that relate to the Democratic People's Republic of Korea (DPRK, also known as North Korea), Iran and to activities relating to chemical weapons.

10. All forms of sanctions imposed by the UK, including UNSCRs and those to satisfy UK foreign and defence goals, are implemented in *the Bailiwick* under *the 2020 Regulations*. *The 2020 Regulations* give automatic effect in *the Bailiwick* to sanctions regimes enacted by the UK under the Sanctions Act.

11. Notwithstanding *the Bailiwick's* independent sanctions regime, trans-jurisdictional issues may arise at times. Many transfers of *funds* will be made to or from another jurisdiction that operates a sanctions regime and in such cases a licence, authorisation, or notification may be required in both jurisdictions.

12.3. Extra-Territorial Sanctions

12. Whilst not directly enforceable in *the Bailiwick*, the legislative frameworks of some jurisdictions such as the US and EU contain provisions which have extra-territorial effect, so that they may apply to some of the parties involved in a *Bailiwick* transaction on the grounds of nationality or place of incorporation even if the jurisdiction in question is not involved in that transaction. The firm may also find the US and EU sanctions lists useful source material to identify persons potentially connected *TF*. The US and EU provisions are summarised below.

13. OFAC regulations apply to any persons or entities, wherever based, trading in US Dollars, as well as:

   (a) US citizens and permanent resident immigrants regardless of where they are located;
   (b) persons and entities within the US;
   (c) US incorporated entities and their foreign branches;
   (d) in the cases of certain sanctions, such as those regarding Cuba and North Korea, all foreign subsidiaries owned or controlled by US companies; and
   (e) in certain cases, foreign persons in possession of US origin goods.

14. EU sanctions apply to nationals of members states and any activity within a member state.

12.4. Administration of the Bailiwick's Sanctions Regime

15. The administration of *the Bailiwick's* sanctions regime is the responsibility of the States of Guernsey Policy and Resources Committee. The Commission has responsibility for supervising firms' compliance with sanctions which apply in *the Bailiwick.*

12.5. Obligation to Report

16. Under the Sanctions (Bailiwick of Guernsey) Law, 2018 ("the Sanctions Law"), there are specific reporting obligations which the firm must comply with. *The Bailiwick's* reporting obligations are outlined on the States of Guernsey's website. Under *the Terrorist Asset-Freezing Law* and *the Sanctions Law*, it is a criminal offence for the firm to fail to disclose to the Policy and Resources Committee any knowledge or suspicion it may have that a *customer* or potential *customer* is a designated person or has committed any of the offences set out in *the Terrorist Asset-Freezing Law* or *the Sanctions Law*. This requirement is in addition to the reporting obligations in *the Disclosure Law* and *the Terrorism Law*. A guidance note issued by the States of Guernsey Policy and Resources Committee regarding reporting obligations can be found through the following link

https://www.gov.gg/CHttpHandler.ashx?id=173751&p=0

17. The firm should be aware that the effects of failing to comply with sanctions orders could have serious repercussions. This could include prosecution for criminal offences and/or financial penalties, levied not only against the firm, but potentially also personally against the senior management of the firm. Any such prosecution is likely to result in extensive reputational damage for the firm, its *board* and *the Bailiwick* as an international finance centre.

12.6. Sanctions Measures and Targets

18. Information on sanctions measures in place with listed regimes may be found on the States of Guernsey's website at:

https://www.gov.gg/sanctionsmeasures

19. A consolidated list of financial sanctions targets can be found at HM Treasury's website at:

https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets

12.7. Licences

20. A licence is a written authorisation from a named competent authority to allow an activity which would otherwise be prohibited by sanctions measures. Under *the 2020 Regulations* and the *Terrorist Asset-Freezing Law*, *the Bailiwick* competent authority for licences in respect of financial services and related matters is the States of Guernsey Policy & Resources Committee.

21. All applications for licences should be addressed to the Regulatory and Financial Crime Policy Team of the States of Guernsey Policy & Resources Committee in the first instance. Further information regarding licences may be found on the States of Guernsey website at:

https://www.gov.gg/CHttpHandler.ashx?id=103136&p=0

12.8. Policies, Procedures and Controls

22. The firm must have in place appropriate and effective policies, procedures and controls to identify, as soon as practicable, whether a prospective or existing *customer*, *beneficial owner* and other *key principals*, is a sanctioned person or is linked to a sanctioned person as defined in the *Sanctions Law* and/or a designated person as defined in *Terrorist Asset-Freezing Law.*

23. All listings (or changes to listings) made by the UN are automatically and immediately effective under UK sanctions regimes as soon as they are made. The same is true of autonomous UK listings (or changes to listings). These listings or changes are therefore also automatically and immediately effective under *the Bailiwick's* legal framework (and the same would apply to any listings or changes to listings made by the States of Guernsey Policy & Resources Committee). This means in turn that the legal obligation on firms to comply with a new listing takes immediate effect when the listing is made, without the need for any legislation or other measures (e.g. notifications) to be taken by *the Bailiwick* authorities. Therefore, it is imperative that firms take steps to ensure that they are aware of new listings (or changes to listings) as soon as they are made.

24. For the purposes of *Commission Rule* 12.22 specified businesses should refer to the lists published by the UN and by HM Treasury. HM Treasury maintains a list which includes all persons whose designations are effective in *the Bailiwick* (including designations by the UN), other than those persons specifically designated by the States of Guernsey Policy and Resources Committee under *the Terrorist Asset-Freezing Law*. Lists of sanctioned persons which apply in the Bailiwick can be found through the below links:

www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets

www.gov.gg/sanctionsmeasures

25. The UN and UK provide a notification facility for advising when the lists of designated persons maintained by them are updated to which the firm should subscribe. For updates of the UN list, an email may be sent to *sc-sanctionslists@un.org* requesting to subscribe to the mailing list of updates to UN designations. HM Treasury link is:

public.govdelivery.com/accounts/UKHMTREAS/subscriber/new

26. The *FIU* also issues notices about new listings and changes to listings via its THEMIS system on behalf of the Policy & Resources Committee. Firms which are not already registered to receive THEMIS updates from the *FIU* should do so via this link:

https://guernseyfiu.gov.gg/article/175901/Contact

27. In addition, as referenced previously, OFAC sanctions apply to all transactions in US Dollars. Therefore where the firm is party to such a transaction it should be mindful of the US sanctions regime. OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups and entities, such as terrorists and narcotics traffickers designated under programmes that are not country specific. Collectively such individuals and companies are called Specially Designated Nationals ("SDNs"). The assets of SDNs are blocked and US entities are prohibited from dealing with them. The list of SDNs, and a free OFAC search facility, can be found through the below links:

www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx

sanctionssearch.ofac.treas.gov/

28. The firm must have appropriate and effective policies, procedures and controls to detect and block transactions connected with a sanctioned person or linked to a sanctioned person as defined in *Sanctions Law* and/or a designated person as defined in *the Terrorist Asset-Freezing Law*.

29. The transaction monitoring systems and/or controls used should enable the firm to identify:

(a) transactions, both incoming and outgoing, involving sanctioned/designated persons; and
(b) where the firm is a *bank, VASP* or *PSP*, transactions where insufficient identifying information has been provided in accordance with the *wire transfer* or *virtual asset transfer* requirements, potentially for the purpose of circumventing sanctions monitoring controls (see Chapters 14 and 18 of this *Handbook*).

12.9. Customer Screening

30. In order to comply with *Commission Rule* 12.28 above, as a minimum the firm should undertake sanctions screening for all new *business relationships* and *occasional transactions*, including the *customer*, *beneficial owner* and other *key principals*, at the time of take-on, during periodic reviews and when there is a trigger event generating a relationship review.

31. Following changes to the lists of persons designated by the UN or UK, the States of Guernsey Policy and Resources Committee will issue sanctions notices to alert firms to such changes. These sanctions notices are issued by the *FIU* via THEMIS and *the Commission* through its website.

mlro.gov.gg

www.gfsc.gg/news/sanctions

32. The firm should have appropriate policies, procedures and controls in place to ensure that the content of such notices is reviewed without delay, including a comparison of the firm's *customer* base against the sanctioned/designated persons listed within the notices. Where a positive match is identified the firm should ensure that the requisite report is filed in accordance with the legislation relevant to the particular sanctions notice.

33. Where the firm utilises an automated method of sanctions screening, the firm should maintain, or have access to, an audit trail of the screening conducted by the system. The audit trail should enable the firm to demonstrate the dates on which screening checks have been undertaken and the results of those checks, thus allowing the firm to *satisfy* itself, and demonstrate to third parties, that the system is operating effectively. Where the firm is part of a wider group and utilises a group-wide screening system, the firm should seek written confirmation from its head office that such an audit trail exists and that the firm can have access to any specific records upon request.

12.10. Compliance Monitoring Arrangements

34. The firm must ensure that its compliance monitoring arrangements include an assessment of the effectiveness of the firm's sanctions controls and their compliance with *the Bailiwick's* sanctions regime.

35. Testing undertaken in respect of any sanctions screening system should cover the following:

(a) ensuring that the screening system has been correctly configured and that the relevant pre-set rules have been activated;
(b) assessing the accuracy of the screening system or method utilised, for example, through an analysis of the alerts generated, to ensure that designated persons are promptly identified;
(c) determining the appropriateness of the firm's controls for the business undertaken, including the method and frequency of testing;
(d) where upgrades have been applied, ensuring that the system performs as expected;
(e) where reliance is placed upon a third party for sanctions screening, the firm should verify the effectiveness of the screening being undertaken by that party; and

(f) determining the appropriateness of the action taken by the firm where a sanctions match has been identified to ensure that the *proceeds* associated with designated persons are controlled and the necessary reporting undertaken in compliance with applicable regulatory requirements.

36. As part of its compliance testing, the firm should give consideration to assessing the sensitivity of any screening tools used, i.e. testing the system's 'fuzzy logic'. Such tests could be conducted by using real-life case studies, entering the name of sanctioned natural or *legal persons* to ensure that the expected results are achieved. Results of this testing would be expected to form part of the management reporting on the firm's compliance monitoring programme as set out under section 2.4.2 of the Handbook.

12.11. Reporting to the Commission

37. As soon as practicable after it has met the statutory reporting requirements to the States of Guernsey Policy and Resources Committee under the *Sanctions Law* and *the Terrorist Asset-Freezing Law*, the firm must provide a report to the Commission, setting out as a minimum:

(a) the name of the *customer*, *beneficial owner*, *key principal* or the transaction and/or asset linked to a sanctioned/designated person; and
(b) the nature of the *business relationship* or *occasional transaction*, including the transaction and/or asset value.

12.12. Record Keeping

38. The firm must maintain a register recording all reports made to the States of Guernsey Policy and Resources Committee associated with a sanctioned/designated person. The register must include, as a minimum:

(a) the nature of the report made;
(b) the transaction and/or asset values associated with the sanctioned/designated person at the time of the designation;
(c) details of the controls in place to ensure that the sanctioned/designated person or linked assets are frozen; and
(d) if relevant, details of any licenses sought from the States of Guernsey Policy and Resources Committee.

39. The recording of adequate and appropriate information regarding the firm's exposure to sanctions is beneficial in helping the firm understand and mitigate its *TF* and *PF* sanctions *risk* under Paragraph 2 of *Schedule 3*, and will assist the firm in maintaining compliance with both the *Sanctions Law* and *the Terrorist Asset-Freezing Law*.

40. The information in the register as set out in Rule 12.38 may also assist the *board* of the firm in discharging its responsibilities under Paragraph 15(1) of *Schedule 3*, therefore the *board* should be provided with regular management information on the firm's exposure to sanctions.

Chapter 13
Reporting Suspicion

Contents of this Chapter

13.1. Introduction

1. This Chapter outlines the statutory provisions concerning the disclosure of information; the policies, procedures and controls necessary for reporting and disclosing suspicion; and the provision of information for the purposes of the reporting and disclosing of suspicion.

2. The obligations to report and disclose suspicion are set out within *the Disclosure Law* and *the Terrorism Law* (together "*the Reporting Laws*"). Additional obligations are set out in the Disclosure (Bailiwick of Guernsey) Regulations, 2007 as amended ("*the Disclosure Regulations*"), the Terrorism and Crime (Bailiwick of Guernsey) Regulations, 2007 as amended (together "*the Reporting Regulations*"), the Disclosure (Bailiwick of Guernsey) (Information) Regulations, 2019 as amended and the Terrorism and Crime (Bailiwick of Guernsey) (Information) Regulations, 2019 as amended (together "*the Information Regulations*"), together with *Schedule 3*.

3. References in this Chapter to suspicion are references to suspicion that another person is engaged in *ML, TF* or *PF*, or that certain property is, or is derived from, the *proceeds* of criminal conduct or terrorist property, as the case may be.

4. References in this Chapter to criminal conduct are references to any conduct which constitutes a criminal offence under the law of any part of *the Bailiwick*, or is, or corresponds to, conduct which, if it all took place in any part of *the Bailiwick*, would constitute an offence under the law of that part of *the Bailiwick*.

5. References in this Chapter to *ML* are references to offences under Sections 38, 39 and 40 of *the Law* or Part IV of the Drug Trafficking (Bailiwick of Guernsey) Law, 2000 as amended ("*the Drug Trafficking Law*").

6. The overall purpose of Sections 38, 39 and 40 of *the Law* and Part IV of *the Drug Trafficking Law* is to create extremely wide ranging 'all crime' prohibitions on *ML*, covering the following activities:

   (a) concealing or transferring the *proceeds* of criminal conduct or drug trafficking;
   (b) assisting another person to retain the *proceeds* of criminal conduct or drug trafficking; and
   (c) the acquisition, possession or use of the *proceeds* of criminal conduct or drug trafficking.

7. References in this Chapter to *TF* are references to offences under Sections 8, 9, 10 or 11 of *the Terrorism Law*, Sections 9, 10, 11, 12 or 13 of *the Terrorist Asset-Freezing Law* or under Ordinances implementing international sanctions measures in respect of terrorism that are listed at Section 79 of *the Terrorism Law*. These offences apply not only to the financing of terrorist acts, but also to the financing of terrorist organisations, or individual terrorists, even in the absence of a link to a specific terrorist act or acts. The offences cover the following activities:

   (a) fund raising for the purpose of terrorism;
   (b) using or possessing money or other property that is intended to be, or may be, used for the purposes of terrorism;
   (c) funding arrangements for the purposes of terrorism;
   (d) money laundering of terrorist property; and
   (e) making *funds* or other economic resources available to persons included in terrorism-related sanctions lists.

8. References in this Chapter to *PF* are references to offences under Sections 8, 9, 10, 11 and 66 of *the Terrorism Law*, Sections 38, 39 and 40 of *the Law* and Section 5 of the Explosive Substances Law, 1939 or under Ordinances implementing any international sanctions measure that has been

implemented in *the Bailiwick* and relate to the proliferation of weapons of mass destruction and its financing. The offences cover the following activities:

(a) ancillary offences (aiding and abetting etc) in respect of activity outside the Bailiwick relating to biological, chemical or nuclear (including radiological) weapons;
(b) offences relating to the financing of terrorism, as the definition of terrorism could encompass activities relating to proliferation;
(c) offences in connection with the acquisition, possession, use, transfer, concealment or retention of proceeds of criminal conduct, which could include proliferation and proliferation financing activities; and
(d) offences in respect of any person who by the supply of or solicitation for money, the providing of premises, the supply of materials, or in any manner whatsoever procures, counsels, aids, abets or is accessory to the commission of any crime under *the Terrorism Law*.

9. The *ML* and *PF* offences in Sections 38 to 40 of *the Law* and Part IV of *the Drug Trafficking Law* are expressed as not applying to acts carried out with the consent of a *police officer*, where that consent is given following a disclosure of suspicion. The same applies in respect of the *TF* and *PF* offences at Sections 8 to 11 and 66 of *the Terrorism Law*. The effect of these provisions is that if, following the making of a report and disclosure of suspicion under *the Reporting Laws*, the *FIU* consents to the firm or person in question carrying out a relevant act, the firm or person will have a defence to a possible charge of *ML*, *TF* or *PF*, as the case may be, in relation to that act. This is referred to informally as the consent regime on which the *FIU* has issued guidance.

https://guernseyfiu.gov.gg/CHttpHandler.ashx?id=167136&p=0

10. Pursuant to *the Reporting Regulations*, the firm shall report and disclose suspicion to the *FIU* using the prescribed manner, specifically the online reporting facility THEMIS. Further information on the form and manner of disclosing suspicion can be found in Section 13.8. of this Chapter.

11. The firm should note that the court will take account of the *Commission Rules* and *guidance* provided in this *Handbook* in considering compliance with the disclosure requirements of *the Reporting Laws*, *the Reporting Regulations* and *Schedule 3*.

12. References in this Chapter to a transaction or activity include an attempted or proposed transaction or activity, or an attempt or proposal to enter into a *business relationship* or undertake an *occasional transaction*.

13.2. Definition of Knowledge or Suspicion

13. *The Reporting Regulations* do not define suspicion, though there is a body of UK case law which has been applied in *the Bailiwick* and which can assist *employees* of the firm in determining if there is sufficient knowledge or suspicion to file an internal disclosure with the *MLRO*, and in turn assist the *MLRO* in determining whether to make an external disclosure to the *FIU*.

14. In the case of R v Hilda Gondwe Da Silva[1], the following was considered to amount to suspicion:

> 'there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice. But the statute does not require the suspicion to be 'clear' or 'firmly grounded and targeted on specific facts', or based upon 'reasonable grounds''.

[1] R v Hilda Gondwe Da Silva [2006] 2 Crim App R 35

15. In the case of Shah v HSBC[2], the English High Court took the view that there is a very low threshold for suspicion, which does not have to be either reasonable or rational.

16. The English courts have therefore defined suspicion as beyond mere speculation, being based on some substance. It is something less than personal or subjective knowledge and does not require proof based on firm evidence. The individual filing a disclosure must think there is a possibility, more than merely fanciful, that the relevant facts exist and the suspicion must be of a settled nature, i.e. more than an 'inkling' or 'fleeting thought'.

13.3. Obligation to Disclose

17. In accordance with the requirements of *the Reporting Laws*, all suspicious transactions and activity, including attempted transactions and activity, are to be reported regardless of the value of the transaction.

18. A suspicion may be based upon:

    (a) a transaction or attempted transaction or activity which is inconsistent with a *customer's* (or *beneficial owner's*) known legitimate business, activities or lifestyle or is inconsistent with the normal business for that type of product/service; or
    (b) information from other sources, including law enforcement agencies, other government bodies (for example, Income Tax), the media, intermediaries, or the *customer* themselves.

19. An important precondition for the recognition of suspicious activity is for the firm to know enough about the *business relationship* or *occasional transaction* to recognise that a transaction or activity is unusual in the context. Such knowledge would arise mainly from complying with the monitoring and on-going *CDD* requirements in Paragraph 11 of *Schedule 3* and Chapter 11 of this *Handbook*.

20. The *board* of the firm and all *employees* should appreciate and understand the significance of what is often referred to as the objective test of suspicion. It is a criminal offence for anyone employed by the firm to fail to report where they have knowledge, suspicion, or reasonable grounds for knowledge or suspicion, that another person is laundering the *proceeds* of any criminal conduct or is carrying out *terrorist financing* or *proliferation financing*.

21. What may constitute reasonable grounds for knowledge or suspicion will be determined from facts or circumstances from which an honest and reasonable person employed by the firm would have inferred knowledge or formed the suspicion that another was engaged in *ML, TF* or *PF*.

22. A transaction or activity which appears unusual is not necessarily suspicious. An unusual transaction or activity is, in the first instance, likely to be a basis for further enquiry, which may in turn require judgement as to whether it is suspicious. As an example, an out of the ordinary transaction or activity within a *business relationship* should prompt the firm to conduct enquiries about the transaction or activity.

23. There may be a number of reasons why the firm is not entirely happy with *CDD information* or where the firm otherwise needs to ask questions. Examples of such are provided within Section 13.5. of this Chapter. Where the firm has queries, regardless of the level of suspicion, to assist them in formulating or negating a suspicion, any enquiries of the *customer* or other *key principal* should be made having due regard to the tipping off provisions.

24. The firm should consider whether the nature of a particular suspicion is such that all of the assets of the *business relationship* are potentially suspect. Where it is not possible to separate assets

[2] Shah v HSBC Private Bank (UK) Limited [2012] EWHC 1283

which are suspicious from those which are legitimate, it will be necessary to carefully consider all future transactions or activity and the nature of the continuing relationship. The firm should also consider implementing an appropriate *risk*-based strategy to deal with any *risk* associated with the *business relationship*.

25. It should be noted that suspicion of *ML*, *TF* or *PF* could relate to assets whether they directly or indirectly relate to criminal conduct.

26. While the firm is not expected to conduct the kind of investigation carried out by law enforcement agencies, it must act responsibly when asking questions to satisfy any gaps in its *CDD*, or its understanding of a particular transaction or activity or proposed transaction or activity.

27. Due to its relationship with the customer, the firm is best placed to ask questions the answers to which could negate suspicions, and should generally do so before deciding whether to report a suspicion.

13.4. Attempted Transactions

28. The definition of *ML*, *TF* and *PF* in *the Reporting Laws* includes an attempt to carry out an offence of *ML*, *TF* or *PF*. This means that attempted transactions fall within the scope of the reporting obligations. An attempted transaction could be classified as one that a *customer* intended to conduct with the firm and took some form of action or activity to do so but failed to complete. An attempted transaction is different from a single request for information, such as an enquiry as to the fee applicable to a specific transaction. The *customer* must enter into negotiations or discussions with the firm to conduct the transaction or activity and such activity must involve specific measures to be taken by either the *customer* or the firm.

29. The obligation to report suspicion applies to all types of activity and attempted transactions or activity, including circumstances where there is no existing *business relationship* with the *customer* and no such *business relationship* is subsequently established.

30. During the course of attempting to set up a new *business relationship*, due consideration should be given during the *CDD* process to key points raised with or by the *customer*, for example, if the *customer* fails to explain the source of *funds*; if the purpose of the *account* or advice required does not make sense; or if questions are asked about the disclosure to tax authorities of the existence of an *account* or the disclosure to other similar authorities. Depending upon the information received, the firm may form a suspicion of *ML*, *TF* and/or *PF* in which case a disclosure shall be submitted to the *FIU* in accordance with *the Disclosure Law* or *the Terrorism Law*.

31. The *FIU* has published a guidance document concerning 'Attempted Transactions'. The objective of the document is to assist firms in the determination of whether a disclosure should be submitted to the *FIU*.

https://guernseyfiu.gov.gg/article/176702/FIU-Guidance

13.5. Potential Red Flags

32. The following is a non-exhaustive list of possible *ML*, *TF* and *PF* red flags that the firm should be mindful of when dealing with a *business relationship* or *occasional transaction*:

(a) The deposit or withdrawal of unusually large amounts of cash from an *account*.
(b) Deposits or withdrawals at a frequency that is inconsistent with the firm's understanding of that *customer* and their circumstances.

(c) Transactions involving the unexplained movement of *funds*, either as cash, *virtual assets* or *wire transfers*.
(d) Payments received from, or requests to make payments to, unknown or un-associated third parties.
(e) Personal and business related money flows that are difficult to distinguish from each other.
(f) Financial activity which is inconsistent with the legitimate or expected activity of the *customer*.
(g) An *account* or *business relationship* becomes active after a period of dormancy.
(h) The *customer* is unable or reluctant to provide details or credible explanations for establishing a *business relationship*, opening an *account* or conducting a transaction.
(i) The *customer* holds multiple *accounts* for no apparent commercial or other reason.
(j) *Bank* drafts cashed in for foreign currency.
(k) Cash deposited domestically with the *funds* subsequently withdrawn from ATMs in another jurisdiction.
(l) Early surrender of an insurance policy incurring substantial loss.
(m) Frequent early repayment of loans.
(n) Frequent transfers indicated as loans sent from relatives.
(o) *Funds* transferred to a charity or NPO with suspected links to a terrorist organisation.
(p) High level of *funds* placed on store value cards.
(q) Insurance policy being closed with a request for the payment to be made to a third party.
(r) Large amounts of cash from unexplained sources.
(s) Obtained loan and repaid balance in cash.
(t) Purchase of high value assets followed by immediate resale with payment requested via cheque.
(u) Request by a third party (outside of *the Bailiwick*) to pay cash (in excess of €10,000) for purchase of high value assets, for example, vehicles.
(v) *Funds* transferred directly, or indirectly to a third party with suspected links, to the Democratic People's Republic of Korea or Iran.
(w) Inconsistencies or irregularities within contracts, invoices, credit notes or trade documents (for example, bill of lading, bill of sale, promissory notes etc).

33. The above list is not exhaustive and its content is purely provided to reflect examples of possible red flags. The existence of one or more red flags does not automatically indicate suspicion and there may be a legitimate reason why a *customer* has acted in the manner identified.

13.6. Policies, Procedures and Controls

34. In accordance with Paragraph 12(1)(h) of *Schedule 3*, the firm shall ensure that it establishes and maintains such other appropriate and effective procedures and controls as are necessary to ensure compliance with requirements to make disclosures under Part I of *the Disclosure Law*, and Sections 15 and 15A or Section 12 (as appropriate) of *the Terrorism Law*.

35. In establishing appropriate and effective policies, procedures and controls to facilitate compliance with the requirements of *the Reporting Laws* and *the Reporting Regulations*, the firm's policies, procedures and controls must ensure that:

(a) Each suspicion of *ML*, TF or *PF* is reported to the *MLRO*, or in his or her absence a *Nominated Officer*, regardless of the amount involved and regardless of whether, amongst other things, it is thought to involve tax matters, in a manner sufficient to satisfy the statutory obligations of the *employee*;
(b) where an *employee* of the firm knows or suspects, or has reasonable grounds for knowing or suspecting, that someone is engaged in *ML, TF* and/or *PF*, an internal disclosure is made to the *MLRO*, or in his or her absence a *Nominated Officer*, of the firm;

(c) the *MLRO* or *Nominated Officer* promptly considers each internal disclosure and determines whether it results in there being knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that someone is engaged in *ML*, *TF* and/or *PF* or that certain property represents, or is derived from, the *proceeds* of criminal conduct, terrorist property or *funds* for proliferation purposes;

(d) where the *MLRO* or *Nominated Officer* has determined that an internal disclosure does result in there being such knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that someone is engaged in *ML*, *TF* and/or *PF*, that the *MLRO* or *Nominated Officer* discloses that suspicion to the *FIU*; and

(e) all internal and external disclosures made in the above manner are of a high quality and meet the standards set out in this *Handbook* and in any feedback and guidance notices issued by the *FIU* and *the Commission*.

13.7. Internal Disclosures

36. In accordance with Paragraph 12(1)(e) *Schedule 3*, the firm shall ensure that where an *employee*, other than the *MLRO*, is required to make a disclosure under Part I of *the Disclosure Law*, or Section 15 or Section 12 (as appropriate) of *the Terrorism Law*, that this is done by way of a report to the *MLRO*, or, in that officer's absence, to a *Nominated Officer*.

37. The firm must have appropriate and effective internal disclosure policies, procedures and controls to ensure that:

(a) all *employees* know to whom within the firm and in what format their suspicions must be disclosed;

(b) all internal disclosures are considered by the *MLRO*, or in his or her absence a *Nominated Officer*, and where the *MLRO* or *Nominated Officer* makes a decision not to make an external disclosure to the *FIU*, the reasons for the decision not to disclose are documented and retained;

(c) enquiries made by an *MLRO* or *Nominated Officer* in respect of disclosures are recorded and documented; and

(d) once an external disclosure has been made to the *FIU*, the *MLRO* or *Nominated Officer* immediately informs the *FIU* where subsequent relevant information or *documentation* is received.

38. The *MLRO* should consider whether to include within the firm's procedures the provision of an acknowledgment to evidence the submission of an internal disclosure. Such an acknowledgement would provide confirmation to the submitter that his or her statutory obligations have been fulfilled.

13.8. Form and Manner of Disclosure to the FIU

39. In accordance with the requirements of *the Reporting Laws*, suspicion of *ML* and *PF* shall be disclosed under the provisions of *the Disclosure Law* and suspicions relating to *TF* shall be disclosed under *the Terrorism Law*.

40. *The Reporting Laws* require that information contained in an internal disclosure made to an *MLRO* or *Nominated Officer* is disclosed to the *FIU* where the *MLRO* or *Nominated Officer* knows or suspects, or has reasonable grounds for knowing or suspecting, as a result of the internal disclosure, that a person is engaged in *ML*, *TF* and/or *PF*.

41. In accordance with Paragraph 12(1)(f) of *Schedule 3*, the firm shall ensure that the *MLRO*, or in that officer's absence a *Nominated Officer*, in determining whether or not he or she is required to

make a disclosure under Part I of *the Disclosure Law*, or Section 15A or Section 12 (as appropriate) of *the Terrorism Law*, takes into account all relevant information.

42. *The Reporting Regulations* provide that disclosures to the *FIU* are to be made in the prescribed manner, specifically through the online reporting facility THEMIS:

mlro.gov.gg

43. In exceptional circumstances a disclosure can be made using the form set out in the Schedule to *the Disclosure Regulations*. However, in accordance with Regulation 1(2) of *the Disclosure Regulations*, the firm shall obtain the consent of an authorised officer (*SIO*, Inspector or above) prior to submitting such a form.

44. In accordance with Paragraph 12(1)(g) of *Schedule 3*, the firm shall ensure that the *MLRO*, or, in his or her absence, a *Nominated Officer*, is given prompt access to any other information which may be of assistance to him or her in considering any report.

45. Prior to making a disclosure to the *FIU*, the firm should consider all available information in respect of the *business relationship* or *occasional transaction*. Notwithstanding this consideration, disclosures to the *FIU* should be made promptly following a determination by the *MLRO* or *Nominated Officer* that a disclosure is appropriate.

46. Where the *MLRO* or *Nominated Officer* considers that a disclosure should be made urgently, for example, where the *customer's* product is already part of a current investigation, initial notification to the *FIU* may be made by telephone on +44(0) 1481 225824.

http://www.guernseyfiu.gov.gg/article/5991/FIU-Contact

13.9. Information to be Provided with a Disclosure

47. The *FIU* has published a guidance document on the Submissions of Suspicious Activity Reports to which reference should be made when considering what information to include within a report. The firm should provide the *FIU* with a full account of the circumstances and grounds (suspected underlying criminality) for suspicion. In providing such detail the firm should include as much relevant information and *documentation* as possible (for example, *CDD information*, statements, contract notes, minutes, transcripts, etc.) to demonstrate why suspicion has been raised and to enable the *FIU* to fully understand the purpose and intended nature of the *business relationship* or *occasional transaction*.

48. The firm should examine all connected *accounts* and/or relationships and provide detailed, current balances of such to the *FIU*. Research of connected *accounts* or relationships should not delay the firm making a disclosure to the *FIU*.

49. *The Reporting Laws* provide that a disclosure made in good faith to a *police officer* does not contravene any obligation as to confidentiality or other restriction on the disclosure of information imposed by statute, contract or otherwise. Additionally, *the Reporting Laws* require that disclosures made under them include information or *documentation* relating to the knowledge, suspicion, or reasonable grounds for suspicion, that the person in respect of whom the disclosure is made is engaged in *ML*, *TF* and/or *PF*, and any fact or matter upon which such knowledge, suspicion, or reasonable grounds for suspicion, is based.

50. The firm is also required to provide the *FIU* with the reasons for suspicion. The firm should clearly define the grounds for suspicion and any specific indicators or suspected criminality

within the main body of the disclosure. The firm may have multiple grounds, i.e. *ML* and tax evasion or bribery and corruption and fraud.

51. For the purposes of the above, 'information' or '*document'* includes any information or *document* relating to:

    (a) any money or property;
    (b) any transaction concerning such money or property; or
    (c) the parties to any such transaction.

52. Where the firm is a legal professional, consideration should be given to Section 13.18. of this *Handbook* which provides guidance in respect of information or *documentation* which may be subject to legal professional privilege.

13.10. Group Reporting

53. It is for each firm or group to consider whether, in addition to any disclosure made in *the Bailiwick*, the *MLRO* should report suspicions within the firm or group, for example, to the compliance department at head office. A report to head office, the parent or group does not remove the requirement to disclose suspicions to the *FIU*.

54. When deciding whether to report within the firm or group, consideration should be given to the sensitivity of the disclosure and the risks involved in the sharing of this information, for example, if the subject of the disclosure is under ongoing investigation by the *FIU*. In this respect, consideration should be given by the firm to anonymising disclosures prior to onward reporting.

13.11. The Response of the FIU

55. Upon submitting a disclosure to the *FIU* via THEMIS, a response acknowledging receipt will be sent automatically. Similarly if, following appropriate permission from the *FIU*, a paper disclosure has been submitted, a response acknowledging receipt will be sent to the firm.

56. If the *FIU* consider that the disclosure, whether through THEMIS or in paper form, contains information that is not of a qualitative nature as detailed in Section 13.9. above, the firm will be notified and sufficient additional information should be provided to the *FIU*.

57. Access to disclosures will be restricted to appropriate authorities and any information provided by the *FIU* emanating from such disclosures will normally be anonymous. In the event of a prosecution, the source of the information will be protected as far as the law allows.

58. In addition, the *FIU* will, so far as is possible, supply on request and through planned initiatives, information as to the current status of any investigations emanating from a disclosure as well as more general information regarding identified trends and indicators.

13.12. Consent Requests

59. It is for each firm, group or person to consider whether any disclosure of suspicion made to the *FIU* concerns an 'act' that would constitute an *ML* offence as detailed in Section 13.1. above.

60. If the firm, group or person suspects such an 'act' may be committed and the firm, group or person intends to carry out such an 'act', a request should be submitted, as part of the firm's disclosure to the *FIU*, outlining the suspected 'act' and seeking consent from a *police officer* to undertake the 'act'.

61. The *FIU* has published a guidance document on the operation of the Consent Regime, to which reference should be made when considering submitting a consent request. In response to a consent request a firm will receive one of five responses:

(a) "Consent regime not applicable" where no suspicion has been identified or no relevant act has been identified.
(b) "Insufficient information" where the suspicious activity report and/or consent request contained insufficient information to enable the *FIU* to arrive at a decision.
(c) "Consent regime not applicable and insufficient information" where both (a) and (b) apply.
(d) "Consent refused" where the *FIU* has not identified any interest of law enforcement in granting consent.
(e) "Consent granted" – which affords a defence to a criminal offence of money laundering in respect of the specified act.

62. The firm, group or person may wish to consider submitting a further disclosure should the circumstances detailed in the original disclosure change in such a way as to give rise to further knowledge or suspicion of *ML* or *FT* not already disclosed to the *FIU*.

63. The *FIU* will endeavour to reply to a consent request as soon as practicable. Nevertheless, it should be noted that the *FIU* is not mandated by law to respond within a specified timeframe. The firm should not continue with the intended transaction or activity until a response from the *FIU* has been received.

13.13. Tipping Off

64. *The Reporting Laws* provide that it is a criminal offence for a person, who knows or suspects that an internal disclosure to an *MLRO* or an external disclosure to the *FIU* has been or will be made, or any information or other matter concerning a disclosure has been or will be communicated to an *MLRO* or the *FIU*, to disclose to any other person information or any other matter about, or relating to, that knowledge or suspicion unless it is for a purpose set out in *the Reporting Laws*.

65. The purposes detailed in *the Reporting Laws* include, but are not limited to, the prevention, detection, investigation or prosecution of criminal offences, whether in *the Bailiwick* or elsewhere.

66. Reasonable enquiries of a *customer*, conducted in a discreet manner, regarding the background to a transaction or activity which has given rise to the suspicion is prudent practice, forms an integral part of *CDD* and on-going monitoring, and should not give rise to tipping off.

67. If the firm identifies open source information on the *customer* (for example, a media article indicating that the *customer* is or has been subject to criminal proceedings) and seeks clarification from the customer this should not give rise to tipping off. However, the firm should consider disclosing the matter to the *FIU* in accordance with Section 13.3. above.

68. HM Procureur has issued a paper entitled 'Guidance on Prosecution for Tipping Off' which specifically permits disclosures to be made to members of the same organisation or linked organisations to discharge their AML and CFT responsibilities, save where there are grounds to believe that this may prejudice an investigation.

http://www.guernseylawofficers.gg/CHttpHandler.ashx?id=116561&p=0

69. The firm's policies, procedures and controls must enable the *MLRO* to consider whether it is appropriate to disclose a suspicion to the *FIU* or to make a request for consent or whether, in assessing the circumstances, it would in the first instance be more appropriate to obtain more information to assist with the decision. Such procedures must also provide for the *MLRO* to

consider whether it would be more appropriate to decline to proceed with a transaction and to give due thought to the future of the *business relationship* as a whole before proceeding.

13.14. Terminating a Business Relationship

70. Whether or not to terminate a *business relationship* is a commercial decision, except where required by law, for example, where the firm cannot obtain the required *CDD information* (see Chapter 4 of this *Handbook* and Paragraph 9 of *Schedule 3*).

71. There will be occasions where it is feasible for the firm to agree a joint strategy with the *FIU*, but the *FIU* will not seek to influence what is ultimately a decision for the firm regarding the future of its *business relationship* with the *customer* and the online reporting facility cannot be used for this purpose.

72. Where the firm takes the decision to terminate a *business relationship* after it has made a disclosure or requested *FIU* consent and is concerned that, in doing so, it may prejudice an investigation or contravene the tipping off obligations, it should engage with the *FIU* accordingly. However, the decision whether or not to terminate a *business relationship* is a decision that ultimately rests with the firm. It may not be possible to terminate a business relationship without committing a money laundering offence.

13.15. FIU Requests for Additional Information

73. Under Regulation 2 of *the Reporting Regulations*, the *FIU* may serve a written notice on a person who has made a disclosure requiring that person to provide additional information relating to the disclosure. Such additional information may provide clarification of the grounds for suspicion and allow the person to whom the disclosure has been made to make a judgement as to how to proceed.

74. Regulation 2A of *the Reporting Regulations* applies where a person has made a disclosure under Section 1, 2 or 3 of *the Disclosure Law* and/or under Section 12, 15 or 15C of *the Terrorism Law* and the *police officer* to whom the disclosure was made believes, as a result, that a third party may possess relevant information.

75. A *police officer* may, by notice in writing served upon a third party, require that third party to provide the *police officer* or any other specified officer with such additional information relating to the initial disclosure as it may require. Any such additional information will be requested in writing.

76. Under Regulation 2 of *the Information Regulations* a police officer may, by notice in writing served upon a party, require that party to provide the police officer or any other specified officer with information in cases where no disclosure has been made, but in response e.g. to an enquiry from a domestic or international competent authority.

77. Ordinarily the information requested under Regulation 2 or Regulation 2A of *the Reporting Regulations* or under *the Information Regulations* shall be provided within seven days, though the *FIU* may extend that time period when justification is provided by the firm regarding the need to extend the period. The time period may also be reduced if the information is required urgently.

78. The firm has a statutory obligation to provide additional information pursuant to Regulation 2 or Regulation 2A of *the Reporting Regulations*. The *police officer* would have obtained authority from the Head of the *FIU*, the Director of the *EFCB* or such person the Director of the *EFCB* may authorise for this purpose, or an officer of the rank of *SIO* or Inspector (or above) for a notice

to be served. Failure without reasonable excuse to comply with a notice (including within the specified time frame) is a criminal offence.

13.16. Management Information

79. The regular receipt of adequate and appropriate MI is beneficial in helping the *board* ensure that the firm can discharge its responsibilities fully under Paragraph 12(1)(h) of *Schedule 3*.

80. The MI provided to the *board* must include, as a minimum:

(a) the number of internal disclosures received by the *MLRO* or a *Nominated Officer*;
(b) the number of external disclosures reported onward to the *FIU*;
(c) an indication of the length of time taken by the *MLRO* or *Nominated Officer* in deciding whether or not to externalise an internal disclosure; and
(d) the nature of the disclosures.

13.17. Record Keeping

81. In accordance with *Commission Rule* 16.17., in addition to the record keeping requirements in respect of individual disclosures, the firm must also maintain a register recording all internal and external disclosures to allow for the *MLRO* to maintain oversight of matters. This will assist in, amongst other things, identifying trends in internal and external disclosures and vulnerabilities across the firm's *customer* base.

13.18. Legal Professional Privilege and Privileged Circumstances

13.18.1. Introduction

82. There may be times when there are tensions between lawyers' professional and ethical obligations to their *customers* and their reporting obligations under *the Reporting Laws*, t*he Reporting Regulations* and *Schedule 3*. Lawyers are subject to unique ethical and legal obligations that mean that in limited circumstances they may be restricted in their ability to disclose a suspicion of *ML*, *TF* or *PF*. The concept of legal professional privilege ("LPP") recognises a *customer's* fundamental human right to be candid with his or her legal adviser, without fear of later disclosure to his or her prejudice.

83. Section 3(6)(c)-(d) of *the Disclosure Law* and Sections 12(6)(c)-(d) and 15(6)(a)-(b) of the *Terrorism Law* recognise that there may be limited circumstances in which a failure to report may be excused by providing that a person does not commit an offence for failing to disclose a suspicion of *ML*, *TF* or *PF* where:

(a) he or she has some other reasonable excuse for not disclosing the information or other matter; or
(b) he or she is a professional legal adviser and the information or other matter came to him in privileged circumstances.

84. The same provisions are included in the equivalent UK legislation and at the time of publication of this *Handbook* there is no judicial guidance (either in the UK or *the Bailiwick*) on what might constitute a 'reasonable excuse' under Section 3(6)(c) of *the Disclosure Law* and Sections 12(6)(c) and 15(6)(a) of *the Terrorism Law* referenced above.

85. Whilst it will ultimately be for the courts to decide if a reason for not making a disclosure was a reasonable excuse, *the Commission* agrees with the position taken by the UK Legal Sector

Affinity Group[3] that a person will have a reasonable excuse for not making an authorised disclosure when the knowledge or suspicion of *ML*, *TF* or *PF* is based on privileged information and LPP is not excluded by the exceptions set out below.

86. In any given case a person should clearly document his or her reasons for concluding that there is a reasonable excuse for non-disclosure.

87. As noted above, distinct from LPP, in accordance with Section 3(6)(d) of *the Disclosure Law* and Sections 12(6)(d) and 15(6)(b) of *the Terrorism Law*, a legal professional adviser may also have a defence from prosecution for failure to report where information or another matter giving rise to knowledge or suspicion of *ML*, *TF* of *PF* 'came to him in privileged circumstances'.

88. *The Reporting Laws* in turn state that information or another matter comes to a professional legal adviser in privileged circumstances if it is communicated or given to them:

    (a) by (or by a representative of) a *customer* in connection with the provision of legal advice;
    (b) by (or by a representative of) a person seeking legal advice; or
    (c) by a person in connection with legal proceedings or contemplated legal proceedings.

89. Neither LPP nor the privileged circumstances exemption will apply if the information is communicated or given to the legal professional with the intention of furthering a criminal purpose.

90. The remainder of this Section examines the tension between a legal professional's duties and the provisions of *the Reporting Laws* and *the Reporting Regulations* and should be read in conjunction with the rest of this Chapter. If you are still in doubt as to your position, you should seek independent legal advice.

13.18.2. Overview of LPP

91. LPP is a privilege against disclosure, ensuring *customers* know that certain *documents* and information provided to legal professionals cannot be disclosed at all. It recognises the *customer's* fundamental human right to be candid with his or her legal adviser, without fear of later disclosure to his or her prejudice. It is an absolute right and cannot be overridden by any other interest.

92. LPP does not, however, extend to everything legal professionals have a duty to keep confidential. LPP protects only those confidential communications falling under either (or both) of the two heads of privilege – advice privilege or litigation privilege.

93. LPP belongs to the *customer*, not the legal professional, and may only be waived by the *customer*.

13.18.3. Advice Privilege

94. Communications between a legal professional adviser, acting in his or her capacity as a legal professional, and his or her *customer*, are privileged if they are both:

    (a) confidential; and
    (b) made for the dominant purpose of seeking legal advice from a legal professional or providing legal advice to a *customer*.

[3] The group of AML supervisors for the UK legal sector. *The Commission's* position as set out here is based on guidance issued by the UK Legal Sector Affinity Group in March 2018: https://www.lawsociety.org.uk/policy-campaigns/articles/anti-money-laundering-guidance/.

95. Communications are not privileged merely because a *customer* is speaking or writing to a legal professional. The protection applies only to those communications that directly seek or provide advice, or which are given in a legal context, that involves the legal professional using his or her legal skills and which are directly related to the performance of the legal professional's professional duties.

13.18.4. Litigation Privilege

96. Litigation privilege, which is wider than advice privilege, protects confidential communications made after litigation has started, or is reasonably in prospect, between any of the following:

(a) a legal professional and a *customer*;
(b) a legal professional and an agent, whether or not that agent is a legal professional; or
(c) a legal professional and a third party.

97. These communications are to be for the sole or dominant purpose of litigation, for any of the following:

(a) seeking or giving advice in relation to it;
(b) obtaining evidence to be used in it; or
(c) obtaining information leading to obtaining such evidence.

13.18.5. Important Points to Consider with LPP

98. An original *document* not brought into existence for privileged purposes and so not already privileged, does not become privileged merely by being given to a legal professional for advice or other privileged purpose.

99. Further, where the *customer* of a legal professional is a corporate entity, communication between the legal professional and the employees of a corporate *customer* may not be protected by LPP if the employee cannot be considered to be the *customer* for the purposes of the retainer. As such, some employees will be *customers*, while others will not.

100. It is not a breach of LPP to discuss a matter with the firm's *MLRO* for the purposes of receiving advice on whether to make a disclosure.

13.18.6. Exceptions to LPP

101. LPP protects advice given by a legal professional adviser to a *customer* on avoiding committing a crime or warning them that proposed actions could attract prosecution. LPP does not, however, extend to *documents* which themselves form part of a criminal or fraudulent act, or communications which take place in order to obtain advice with the intention of carrying out an offence. It is irrelevant whether or not the legal professional is aware that they are being used for that purpose.

102. It is not just the *customer's* intention which is relevant for the purpose of ascertaining whether information was communicated for the furtherance of a criminal purpose. It is also sufficient that a third party intends the legal professional/communication to be made with that purpose (for example, where the innocent *customer* is being used by a third party).

103. If the legal professional knows the transaction or activity being worked on constitutes criminal conduct, he or she risks committing an offence by facilitating criminal conduct and/or failing to disclose knowledge or suspicion of *ML*, *TF* or *PF*. In those circumstances, communications relating to the transaction or activity are not privileged and can be disclosed.

104. If the firm merely suspects a transaction or activity might constitute an *ML*, *TF* and/or *PF* offence, the position is more complex. If the suspicions are correct, communications with the *customer* are not privileged. If the suspicions are unfounded, the communications should remain privileged and are therefore not required to be disclosed.

105. LPP will also be lost where there has been an express or implied waiver. This may occur where the communication is no longer confidential, as confidentiality is a requirement for both types of LPP.

13.18.7. Privileged Circumstances

106. Distinct from LPP, and as noted in Paragraph 13.86. above, *the Reporting Laws* both recognise another type of protected communication, one which is received in 'privileged circumstances'. This is not the same as LPP, it is merely an exemption from the requirement to disclose knowledge or suspicion of *ML*, *TF* or *PF*, although in many cases the communication will also be covered by LPP.

107. The essential elements of the privileged circumstances exemption are:

(a) the information or material is communicated to a 'professional legal adviser' (not defined in *the Reporting Laws*):

(i) by a *customer* (or their representative) in connection with the giving of legal advice;
(ii) by a person (or their representative) seeking legal advice; or
(iii) by a person in connection with actual or contemplated legal proceedings; and

(b) the information or material was not communicated or given to the professional legal adviser with a view to furthering a criminal purpose.

108. The exceptions set out in Section 13.18.6. above should be considered when assessing what constitutes furthering a criminal purpose.

13.18.8. Differences Between LPP and Privileged Circumstances

109. Where litigation is neither contemplated nor reasonably in prospect, except in very limited circumstances, communications between a legal adviser and third parties will not generally be protected by LPP.

110. However, the extension of the privileged circumstances concept to cover information communicated by representatives of a *customer* or person seeking legal advice, means that this exemption may apply in circumstances where LPP would not. For example, it may include communications with:

(a) a junior employee of a *customer* (if it is reasonable in the circumstances to consider them to be a representative of the *customer*); or
(b) other professionals who are providing information to the legal adviser on behalf of the *customer* as part of the transaction.

111. The specific facts of each case should be considered when deciding whether or not a person is a representative for the purposes of privileged circumstances, and the legal adviser is encouraged to document this consideration.

112. Confidentiality is also not a necessary element of the privileged circumstances exemption. Disclosure of a communication to a third party may not therefore exclude the application of the privileged circumstances exception in the same way that it would result in LPP being lost.

13.18.9. Making a Disclosure

113. When faced with information or matter that forms the basis of suspicion, it is recommended that a legal professional ask himself the following questions:

    (a) What information would I need to include in a disclosure?
    (b) Is any of that information subject to LPP?
    (c) Did any of that information come to me in 'privileged circumstances'?
    (d) If the answer to (b) and (c) is no, the disclosure should be filed without disclosing any privileged communications;
    (e) If information is subject to LPP and/or came to me in privileged circumstances, has it for any reason lost its privileged status?

        (i) Has LPP been lost due to disclosure?
        (ii) Has the *customer* otherwise waived their LPP?
        (iii) Is there reasonable evidence for me to conclude that the material was communicated to me with a view to furthering a criminal purpose?

    (f) Can I file a coherent disclosure without disclosing the material that came to me in privileged circumstances?

114. If the privileged status has not been lost and a coherent internal disclosure can be filed without disclosing the protected material, a disclosure should be filed on this basis. If privileged status has been lost then the legal professional should disclose the information.

115. In all cases the legal professional should document his or her reasons and ethical considerations which formed the basis of his or her decision whether or not to make a disclosure.

13.19. THEMIS Notices

116. THEMIS has the facility to provide firms with notices which are sent via a generic e-mail address to individual users. These notices are a mechanism through which the *FIU* provides information to all THEMIS users or to specific 'targeted' distribution groups or firms, dependent upon the information or guidance that is being issued.

117. Notices sent via THEMIS include updates on changes to the legislative framework, news of forthcoming presentations or seminars and updates in respect of UK, UN and other sanctions. In addition to generic updates, the *FIU* may specifically 'target' certain distribution groups or firms in respect of a notification that a certain entity or group of entities is under investigation by the *FIU* or other law enforcement agencies. In this respect, THEMIS is the mechanism by which specific 'targeted' notices will be distributed to *MLROs*.

118. The *MLRO* should refer to the THEMIS portal whenever a notification is issued by the *FIU* and additionally at regular intervals on an ad hoc basis. Where targeted notices are issued, the firm should establish if it maintains a *business relationship*, or has conducted an *occasional transaction*, with the entities listed on the notice, or if it has information which may assist the *FIU*. The firm should consider whether the receipt of a targeted notice from law enforcement is sufficient grounds for suspicion to make an external disclosure to the *FIU* in accordance with Section 13.3. of this *Handbook*. It should be noted that the *FIU* have the facility to monitor whether notices have been received and/or read by the recipient.

Chapter 14
Wire Transfers

Contents of this Chapter

14.1. Introduction

1. The Transfer of Funds (Guernsey) Ordinance 2017, along with the parallel ordinances for Alderney and Sark, were brought into force on 26 June 2017 following the EU's enactment of Regulation (EU) 2015/847 on Information Accompanying Transfers of Funds ("*the EU Regulation*") on 20 May 2015. References in this Chapter to "*the Transfer of Funds Ordinance*" should be read as referring to the Transfer of Funds (Guernsey, Sark or Alderney) Ordinance 2017 relevant to the island within which the firm is operating.

2. Article 1 of *the Transfer of Funds Ordinance* gives *the EU Regulation* full force and effect in *the Bailiwick*, subject to certain adaptations, exceptions and modifications as set out in Schedule 1 to *the Transfer of Funds Ordinance*.

3. *The Bailiwick* and the other *Crown Dependencies* have received a derogation enabling *wire transfers* between the *British Islands* to contain the reduced information requirements as compared to those which apply to transfers of funds within the internal market of the EU. The derogation was issued because the EU considered that *the Bailiwick* and the other *Crown Dependencies* had transfer of funds legislation which is equivalent to *the EU Regulation*.

4. Where the firm is a *PSP*, it shall comply with *the Transfer of Funds Ordinance* and should note that in accordance with Article 11 of *the Transfer of Funds Ordinance*, the court will take account of the *Commission Rules* and *guidance* issued by *the Commission* in considering compliance with *the Transfer of Funds Ordinance* and *the EU Regulation*. For the avoidance of doubt, the *Commission Rules* and *guidance* contained in this section have been made in accordance with Article 11 of *the Transfer of Funds Ordinance.*

5. The FATF's principle purposes for developing standards on the *payer* and *payee* information to accompany *wire transfers* are to prevent terrorists and criminals from having unfettered access to *wire transfers* for moving funds and to enable the detection of the misuse of *wire transfers* when it occurs. Key parts of *the FATF Recommendations* include requiring that information about the *payer* and *payee* accompany *wire transfers* throughout the payment chain. This is to ensure the traceability of funds to assist in preventing, detecting and investigating *ML*, *TF* and *PF* and to facilitate the effective implementation of restrictive measures against persons and entities designated under UN and UK sanctions legislation. The standards also require *PSPs* to have appropriate mechanisms for detecting where information is incomplete or missing for the purpose of considering whether it is suspicious and should be reported to the *FIU*.

6. *The Transfer of Funds Ordinance* and *the EU Regulation* require full *customer* information details on the *payer* and certain identity information on the *payee* on all transfers of funds in any currency except where there are derogations from the requirements of *the EU Regulation* which allow for less information about a *payer* and *payee* to accompany a transfer. This Section explains the *payer* and *payee* information that is required and the derogations which permit *PSPs* to effect transfers with reduced levels of information about the *payer* and the *payee* in certain specified circumstances, including transfers between the *British Islands*.

7. *The EU Regulation* sets out the *payer* and *payee* information which shall accompany a transfer and requires both the *PSP* of the *payee* and intermediary *PSP* to have appropriate and effective measures in place to detect when the required *payer* and/or *payee* information is missing or incomplete. *The EU Regulation* also requires that *PSPs* shall have *risk*-based procedures in place to assist where a transfer lacks the required information so as to enable the *PSP* to decide whether to execute, reject or suspend a transfer and to determine the appropriate action to take.

8. *The Transfer of Funds Ordinance* and *the EU Regulation* also introduce increased reporting obligations upon *PSPs* to identify breaches and areas of non-compliance which shall be reported to *the Commission*. *The Transfer of Funds Ordinance* prescribes the manner in which such reports shall be made.

9. Under Article 22 of *the EU Regulation the Commission* is responsible for monitoring compliance with *the EU Regulation.* This includes implementing the measures which are necessary to ensure compliance with those requirements by *PSPs* established in *the Bailiwick*.

10. Parts of this Chapter in clear boxes summarise the requirements of *the EU Regulation* and *the Transfer of Funds Ordinance*. Any paraphrasing of that text within this Chapter represents *the Commission's* own explanation of *the EU Regulation* and *the Transfer of Funds Ordinance* and is for the purposes of information and assistance only. *The Transfer of Funds Ordinance* and *the EU Regulation* remain the definitive texts for the legal requirements upon *PSPs*.

11. As *the Transfer of Funds Ordinance* is based on *the EU Regulation*, *PSPs* may find it of benefit when developing their policies, procedures and controls for *wire transfers* to review guidance issued by the ESAs on the measures *PSPs* should take to detect missing or incomplete information on the *payer* or the *payee* and the procedures they should put in place to manage a transfer of funds lacking the required information.

14.2. Scope

12. The requirements summarised in this Section apply to transfers of funds, in any currency, which are sent or received by a *PSP* or an intermediary *PSP* established in *the Bailiwick*.

13. These requirements do not apply to the transfers set out in Part II of the Schedule to *the Transfer of Funds Ordinance* regarding modification of Article 2 of *the EU Regulation* covering the following transfers:

(a) transfers of funds corresponding to services referred to in points (a) to (m) and (o) of Article 3 of Directive 2007/64/EC of the European Parliament (Directive on Payment Services in the Internal Market). The services referred to in points (a) to (m) and (o) are set out in Paragraph 14.15. below;
(b) transfers of funds carried out using a payment card, electronic money instrument or a mobile phone, or any other digital or information technology ("IT") prepaid or post-paid device with similar characteristics where that card, instrument or device is used exclusively to pay for goods or services and that the number of that card, instrument or device accompanies all transfers flowing from the transaction;
(c) transfers of funds involving the *payer* withdrawing cash from the *payer's* own payment *account*;
(d) transfers of funds to a public authority (construed as to include any Committee of the States or Parochial officers) as payment for taxes, fines or other levies within the *British Islands*;
(e) transfers of funds where both the *payer* and the *payee* are *PSPs* acting on their own behalf; and
(f) transfers of funds carried out through cheque images exchanges, including truncated cheques.

14. It should be noted that the exemption set out in Paragraph 14.13. does not apply when the card, instrument or device is used to effect a person-to-person transfer of funds. Therefore, when a credit, debit or prepaid card is used as a payment system to effect a person-to-person *wire transfer*, the transaction is included within the scope of *the Transfer of Funds Ordinance*.

15. *The EU Regulation* does not apply to the following:

(a) payment transactions made exclusively in cash directly from the *payer* to the *payee*, without any intermediary intervention;

(b) payment transactions from the *payer* to the *payee* through a commercial agent authorised to negotiate or conclude the sale or purchase of goods or services on behalf of the *payer* or the *payee*;

(c) professional physical transport of banknotes and coins, including their collection, processing and delivery;

(d) payment transactions consisting of the non-professional cash collection and delivery within the framework of a non-profit or charitable activity;

(e) services where cash is provided by the *payee* to the *payer* as part of a payment transaction following an explicit request by the payment service user just before the execution of the payment transaction through a payment for the purchase of goods or services;

(f) money exchange business, i.e. cash-to-cash operations, where the funds are not held on a payment *account*;

(g) payment transactions based on any of the following documents drawn on the *PSP* with a view to placing funds at the disposal of the *payee*:

(i) paper cheques in accordance with the Geneva Convention of 19 March 1931 providing a uniform law for cheques;

(ii) paper cheques similar to those referred to in point (i) and governed by the laws of Member States which are not party to the Geneva Convention of 19 March 1931 providing a uniform law for cheques;

(iii) paper-based drafts in accordance with the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;

(iv) paper-based drafts similar to those referred to in point (iii) and governed by the laws of Member States which are not party to the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;

(v) paper-based vouchers;

(vi) paper-based traveller's cheques; or

(vii) paper-based postal money orders as defined by the Universal Postal Union;

(h) payment transactions carried out within a payment or securities settlement system between settlement agents, central counterparties, clearing houses and/or central banks and other participants of the system, and *PSPs*, without prejudice to Article 28 of *the EU Regulation*;

(i) payment transactions related to securities asset servicing, including dividends, income or other distributions, or redemption or sale, carried out by persons referred to in point (h) or by investment firms, credit institutions, collective investment undertakings or asset management companies providing investment services and any other entities allowed to have the custody of financial instruments;

(j) services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, IT and communication network provision, provision and maintenance of terminals and devices used for payment services;

(k) services based on instruments that can be used to acquire goods or services only in the premises used by the issuer or under a commercial agreement with the issuer either within a limited network of service providers or for a limited range of goods or services;

(l) payment transactions executed by means of any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services;

(m) payment transactions carried out between *PSPs*, their agents or branches for their own *account*; or

(n) services by providers to withdraw cash by means of automated teller machines acting on behalf of one or more card issuers, which are not a party to the framework contract with the customer withdrawing money from a payment *account*, on condition that these providers do not conduct other payment services.

14.3. Outgoing Transfers – Obligations upon the PSP of the Payer

14.3.1. Transfers for Non-Account Holders

16. In accordance with Article 4 of *the EU Regulation*, where a transfer of funds is not made from or to an *account* the *PSP* shall obtain *customer* identification information on the *payer* and *payee*, record that information and verify the *customer* information on the *payer*.

17. Where all of the *PSPs* involved in the transfer are established in the *British Islands* and the transfer is of EUR 1,000 or more in a single transaction or in a linked series of transactions which together amount to or exceed EUR 1,000, the transfer shall, in accordance with Article 5(1) of *the EU Regulation*, include a *unique transaction identifier* (which can trace a transaction back to the *payer* and *payee*) for the *payer* and *payee*. If further information (for example, the name and address of the *payer*) is requested by the *PSP* of the *payee* or the intermediary *PSP*, such information shall be provided within three working days of the receipt of a request for such information.

18. Where a transfer is carried out within the *British Islands* which is under the EUR 1,000 threshold, the *customer* identification information on the *payer* and the *payee* shall be obtained and recorded but it is not necessary to verify the *customer* information on the *payer* unless the funds to be transferred have been received in cash or in anonymous electronic money, or the *PSP* has reasonable grounds for suspecting *ML* and/or *FT*.

19. Where a transfer is being made to a *PSP* in any other country or territory, Article 4 of *the EU Regulation* requires that such a transfer include the following *customer* identification information (complete information):

    (a) the name of the *payer*;
    (b) a *unique transaction identifier* (which can trace a transaction back to the *payer*);
    (c) one of either the *payer's* address (residential or postal), national identity number, *customer* identification number or date and place of birth;
    (d) the name of the *payee*; and
    (e) a *unique transaction identifier* which can be traced back to the *payee*.

20. Where the *payer* is an existing *customer* of the *PSP*, the *PSP* may deem verification to have taken place if it is appropriate to do so taking into account the risk of *ML*, *TF* and *PF*.

21. A national identity number should be any government issued personal identification number or other government issued *unique identifier*. Examples of such would include a passport number, national identity card number or social security number.

22. A *customer* identification number may be an internal reference number that is created by a *PSP* which uniquely identifies a *customer* (rather than an *account* that is operated for a *payer* or a transaction) and which will continue throughout a *business relationship*, or it may be a number that is contained within an official document.

14.3.2. Transfers for Account Holders

23. In accordance with Article 4 of *the EU Regulation*, where a *PSP* is seeking to make a transfer from an *account*, the *PSP* shall:

    (a) obtain *customer* identification information on the *payer*, verify that information, and record and retain that information;
    (b) have undertaken *CDD* procedures and retained records in connection with the opening of that *account* in accordance with the requirements of *Schedule 3* and this *Handbook*; and
    (c) obtain information on the identity of the *payee* and the number of the *payee's* payment *account*.

24. Where all of the *PSPs* involved in a transfer are established in the *British Islands*, Article 5 of *the EU Regulation* requires that the transfer includes a payment *account* number of the *payer* and the *payee*. The *account* number could be, but is not required to be, expressed as the IBAN. If further information (for example, the name and address of the *payer*) is requested by the *PSP* of the *payee* or the Intermediary *PSP*, such information shall be provided by the *PSP* within three working days of the receipt of a request for such information.

25. Where a transfer is carried out within the *British Islands* which is under the EUR 1,000 threshold, the *customer* identification information on the *payer* and the *payee* shall be obtained and recorded but it is not necessary to verify the *customer* information on the *payer* unless the funds to be transferred have been received in cash or in anonymous electronic money, or the *PSP* has reasonable grounds for suspecting *ML* and *FT*.

26. Where the *payer* is an existing *customer* of the *PSP*, the *PSP* may deem verification to have taken place if it is appropriate to do so taking into account the *risk* of *ML*, *TF* and *PF*.

27. The permission for transfers, where all *PSPs* involved are established in the *British Islands*, to only include a payment *account* number arises from technical limitations required to accommodate transfers by domestic systems like BACS which are currently unable to include complete information. However, where the system used for such a transfer has the functionality to carry complete information, it would be good practice to include it and thereby reduce the likelihood of inbound requests from *payee PSPs* for complete information.

28. Where the transfer is being made to a *PSP* in any other country or territory, the transfer shall include the following customer identification information:

    (a) the name of the *payer*;
    (b) the *payer's account* number (or IBAN);
    (c) one of either the *payer's* address (residential or postal), national identity number, customer identification number or date and place of birth;
    (d) the name of the *payee*; and
    (e) the *payee's account* number (or IBAN).

29. There may be occasions when the *PSP* of the *payer* does not know the full name of the *payee*. This may arise when the *payer* knows only the surname and the initials of the *payee's* first name(s). In such circumstances it would be acceptable for the *PSP* of the *payer* to use initials with the surname subject to consideration by the *PSP* that the information given by the *payer* on the identity of the *payee* is not misleading and that it is reasonable for the *payer* not to know the full name of the *payee*. The *PSP* of the *payer* should also be mindful that using the initials of the first name(s) of the *payee* may not be accepted by the *PSP* of the *payee*, which could revert with questions on the identity of the *payee* or reject the transfer. The full surname of the *payee* should always be obtained by the *PSP* of the *payer*.

30. In the case of a *payer* that is a company, a transfer must include either the address at which the company's business is conducted or the *customer* identification number of the company.

31. Where the *payer* is a foreign incorporated company administered in *the Bailiwick*, the address referred to in *Commission Rule* 14.30. would be that of its administrator.

32. In the case of a *payer* that is a trust, a transfer must be accompanied by the address of the trustee or the *customer* identification number of the trust.

33. Where a trust has multiple co-trustees, the address referred to in *Commission Rule* 14.32. should be that given to open and maintain the *account*. Where more than one address has been given to open and maintain that *account*, those addresses should be used.

34. *PSPs* must ensure that when messaging systems such as SWIFT MT202 (which provide for transfers where both the *payer* and the *payee* are *PSPs* acting on their own behalf) are used on behalf of another *FSB*, the transfers are accompanied by the *customer* identification information necessary to meet the requirements of *the Transfer of Funds Ordinance*.

14.3.3. Detection of Missing or Incomplete Information

35. Under Article 4 of *the EU Regulation* the *PSP* shall ensure that no transfer is executed before ensuring that the transfer includes the required *customer* identification information on the *payer* and the *payee*.

14.4. Batch Files – Transfers Inside or Outside the British Islands

36. In accordance with Article 6 of *the EU Regulation*, batch files from a single *payer* to multiple *payee*s shall carry the information identified in Paragraph 14.19. of this *Handbook* for the *payer* and that information shall have been verified. However, the individual transfers within the batch file need only carry the *payer's* payment *account* number (or *unique transaction identifier* if there is no *account* number).

37. Where the transfer is under the EUR 1,000 threshold it need only include:

(a) the names of the *payer* and or *payee*; and
(b) the payment *account* numbers of the *payer* and the *payee* or a *unique transaction identifier* if there is no payment *account* for one or both parties.

38. The information requirements of Paragraphs 14.17., 14.24., 14.37. of this *Handbook* are the minimum standards. It is open to *PSPs* to elect to supply complete information with transfers which are eligible for a reduced information requirement and thereby limit the likely incidence of inbound requests for complete information.

14.5. Incoming Transfer – Obligations upon the *PSP* of the *Payee*

39. In accordance with Article 7 of *the EU Regulation* the *PSP* of the *payee* shall obtain *customer* identification information on the *payee*, verify that information and record and retain that information, or to have applied *CDD* measures and retained records in connection with the opening of that *account* in accordance with *Schedule 3* and the *Commission Rules*.

40. Where the *payee* is an existing *customer* of the *PSP*, the *PSP* may deem verification to have taken place if it is appropriate to do so taking into account the *risk* of *ML*, *TF* and *PF*.

41. Articles 7 and 8 of *the EU Regulation* require *PSPs* to have effective policies, procedures and controls for checking that incoming payments contain the required *customer* identification information (which will depend on the location of the *PSPs* involved in the transfer process and the value of the funds being transferred) – see *Commission Rule* 14.63.

14.5.1. Detection of Missing or Incomplete Information

42. PSPs will need to be able to: identify empty message fields; have procedures in place to detect whether the required *customer* identification information is missing on the *payer* or the *payee* (for example, by undertaking sample testing to identify fields containing incomplete information on the *payer* and *payee*); and where information is incomplete, take specified action.

43. SWIFT payments on which mandatory information fields are not completed will automatically fail and the *payee PSP* will not receive the payment. Current SWIFT validation prevents payments being received where the mandatory information on the *payer* and the *payee* is not present at all. However, it is accepted that where the information fields are completed with incorrect or meaningless information, or where there is no *account* number, the payment may pass through the system. Similar considerations apply to non-SWIFT messaging systems which also validate that a field is populated in accordance with the standards applicable to that system (for example, BACS).

44. Under Article 7 of *the EU Regulation* a *PSP* of a *payee* shall have effective policies, procedures and controls:

(a) to detect whether or not the information on the *payer* and the *payee* is complete in accordance with the conventions of the messaging or payment and settlement system being used; and
(b) have effective procedures in place to detect the absence of required information on the *payer* and *payee*.

45. A *PSP* must have in place appropriate and effective policies, procedures and controls to subject incoming payment transfers to an appropriate level of real time and post-event monitoring in order to detect incoming transfers which are not compliant with the relevant information requirements.

46. A *PSP*'s policies, procedures and controls should:

(a) take into account the *ML, TF* and *PF risks* to which it is exposed;
(b) set out which transfers will be monitored in real time and which can be monitored ex-post and why; and
(c) set out what *employees* should do where required information is missing or incomplete.

47. The level of monitoring should be appropriate to the *risk* of the *PSP* being used in connection with *ML, TF* and *PF*, with high *risk* transfers monitored in real time. Consideration should be given to areas such as:

(a) the value of the transaction;
(b) the country or territory where the *PSP* is established and whether that country or territory applies *the FATF Recommendations*, particularly Recommendations 10 (*CDD*); 11 (record keeping) and 16 (*wire transfers*);
(c) the country or territory of the *payer*;
(d) the history of previous transfers with the *PSP* of the *payer*, i.e. whether it has failed previously to comply with the *customer* identification requirement; and
(e) the complexity of the payment chain within which the *PSP* operates.

48. *The Commission* would expect a *PSP*'s ex-post monitoring to include *risk*-based sampling of transfers. Records should be retained and findings periodically reported to the *board* of the *PSP*.

49. Under Article 8 of *the EU Regulation* a *PSP* shall implement effective *risk*-based policies, procedures and controls for determining whether to

(a) reject a transfer; or
(b) execute or suspend the transfer; and

ask for complete information on the *payer* or *payee* before or after crediting the *payee's account* or making funds available to the *payee* on a *risk* sensitive basis where it has identified in the course of processing a transfer that the required information on the *payer* or *payee* is missing or incomplete or if the information fields have been incorrectly filled in.

50. A *PSP* should take a *risk*-based approach when considering the most appropriate course of action to take in order to meet the requirements of Article 8 of *the EU Regulation*. If a decision is made to ask for complete information on the *payer*, a *PSP* should also consider, on the basis of the perceived *risk*, whether to make the payment or to hold the funds until such time as complete information has been received.

51. Where a *payee PSP* becomes aware subsequent to processing the payment that information on the *payer* or *payee* is missing or incomplete either as a result of random checking or other monitoring mechanisms under the *PSP*'s *risk*-based approach, it must seek the complete information on the *payer* and *payee* relevant to the type of transfer it was (either in terms of value or if it was within or outside the *British Islands*).

14.6. Failure to Supply Information

52. Article 8 of *the EU Regulation* also sets out the action required where a *PSP* repeatedly fails to supply information on the *payer* or *payee* required by *the EU Regulation* and reporting obligations. This action may include issuing warnings and setting deadlines, prior to either refusing to accept further transfers from that *PSP* or deciding whether or not to restrict or terminate the *business relationship*.

53. A *PSP* must have appropriate policies, procedures and controls for determining what measures to take when a *PSP* repeatedly fails to provide required information on the *payer* or *payee*.

54. Such policies, procedures and controls should take into account whether the *PSP* is located in a country or territory which has been identified through mutual evaluations or other assessments by the FATF as insufficiently applying *the FATF Recommendations*, particularly Recommendations 10 (*CDD*), 11 (record keeping) and 16 (*wire transfers*).

55. Where the *PSP* has sought complete information on the *payer* and it has not been provided to the *PSP* within a reasonable time frame, the *PSP* must consider, on a *risk*-based approach, the most appropriate course of action to be undertaken.

56. Where a *PSP* of a *payer* is identified as having regularly failed to comply with the information requirements, then the *PSP* of the *payee* must *notify the Commission* of that fact and the steps it has taken to attempt to ensure that such information is supplied.

57. The report to *the Commission* should contain the name and address of the *PSP*, and a summary of the measures taken by the *PSP* of the *payee* to obtain the missing or incomplete information from the *PSP* of the *payer*, including the issuing of warnings or deadlines up until the decision to restrict or terminate the relationship was made.

58. This reporting requirement does not apply to instances where a request for the missing or incomplete information which accompanied a transfer is fulfilled by the *PSP* of the *payer*. The obligation to report applies to circumstances where information requests are not fulfilled and the *PSP* of the *payee* invokes measures which restrict or terminate the *business relationship* with that *PSP*.

14.7. Obligations upon an Intermediary *PSP*

59. In accordance with Article 10 of *the EU Regulation* intermediary *PSPs* (for example, those acting as agents for other *PSPs* or who provide correspondent banking facilities) shall, subject to technical limitations, ensure that all information received on a *payer* and *payee* which accompanies a transfer of funds is retained with the transfer.

60. Under Article 11 of *the EU Regulation* an intermediary *PSP* shall have effective policies, procedures and controls:

(a) to detect whether or not the information on the *payer* and the *payee* is complete in accordance with the conventions of the messaging or payment and settlement system being used; and
(b) have effective procedures in place to detect the absence of required information on the *payer* and *payee*.

61. Under Article 12 of *the EU Regulation* an intermediary *PSP* shall implement effective *risk*-based policies, procedures and controls for determining whether to:

(a) reject a transfer; or
(b) execute or suspend the transfer; and

ask for complete information on the *payer* or *payee* before or after crediting the *payee's account* or making funds available to the *payee* on a *risk* sensitive basis where it has identified in the course of processing a transfer that the required information on the *payer* or *payee* is missing or incomplete or if the information fields have been incorrectly filled in.

62. Article 12 of *the EU Regulation* prescribes the action required where a *PSP* repeatedly fails to supply information on the *payer* or *payee* required by *the EU Regulation* and reporting obligations. This action may include issuing warnings and setting deadlines, prior to either refusing to accept further transfers from that *PSP* or deciding whether or not to restrict or terminate the *business relationship*.

63. An intermediary *PSP* must have appropriate policies and procedures for determining what measures to take when a *PSP* repeatedly fails to provide required information on the *payer* or *payee*.

64. Such policies and procedures should take into account whether the *PSP* which is failing to provide the information is located in a country or territory which has been identified through mutual evaluations or other assessments by the FATF as insufficiently applying *the FATF Recommendations*, particularly Recommendations 10 (*CDD*), 11 (record keeping) and 16 (*wire transfers*).

65. Where a *PSP* is identified as having repeatedly failed to comply with the information requirements, then the intermediary *PSP* must *notify the Commission* of that fact and of the steps it has taken to attempt to ensure that such information is supplied.

66. The report to *the Commission* should contain the name and address of the *PSP* and a summary of the measures taken by the *PSP* of the *payee* to obtain the missing or incomplete information from the *PSP* of the *payer*, including the issuing of warnings or deadlines up until the decision to restrict or terminate the relationship was made.

67. This reporting requirement does not apply to instances where a request for the missing or incomplete information which accompanied a transfer is fulfilled by the *PSP* of the *payer*. The obligation to report applies to circumstances where information requests are not fulfilled and the intermediary *PSP* invokes measures which restrict or terminate the *business relationship* with that *PSP*.

14.8. Reporting

68. *The EU Regulation* and *the Transfer of Funds Ordinance* contain certain reporting requirements upon a *PSP*, whether acting in the capacity of *PSP* of the *payer*, *PSP* of the *payee* or an intermediary *PSP*. Irrespective of the capacity within which the *PSP* is acting there are three distinct reporting requirements which are to report:

(a) missing or incomplete information on a transfer which may give rise to a suspicion which should be reported to the *FIU*;
(b) breaches by a *PSP* of *the EU Regulation* or *the Transfer of Funds Ordinance* to *the Commission*; and
(c) repeated failure by a *PSP* to provide the required *payer* or *payee* information (see Articles 8(2) and 12 (2) of *the EU Regulation* and *Commission Rules* 14.56. and 14.65. above) to *the Commission.*

14.8.1. Reporting Suspicions

69. Articles 9 and 13 of *the EU Regulation* require the *PSP* of the *payee* and an intermediary *PSP* to take into account as a factor missing or incomplete information on the *payer* or the *payee* in assessing whether a transfer of funds or any related transaction is suspicious and whether it should be reported to the *FIU* in accordance with Part I of *the Disclosure Law* and Part II of *the Terrorism Law* and reported in any country affected by the suspicious transfer of funds or related transaction where the *PSP* of the *payee* or intermediary controls both the sending and receiving end of the transfer.

70. In this respect *the Commission* would expect the *PSP*'s internal reporting procedures to apply where an *employee* of a *PSP* forms a suspicion that a transfer may be connected to *ML, TF* and/or *PF*, or that funds are derived from the *proceeds* of crime or terrorist property. For further information on reporting suspicion reference should be made to Chapter 13 of this *Handbook*.

71. *Employees* who are involved in the handling or processing of transfers would be considered *relevant employees* for training purposes and a *PSP* should ensure that its training programme includes training on the requirements of *the EU Regulation* and *the Transfer of Funds Ordinance*, as well as the *PSP*'s policies, procedures and controls on handling transfers of funds and reporting suspicion.

14.8.2. Reporting Breaches

72. Under Article 4 of *the Transfer of Funds Ordinance* a *PSP* shall *notify the Commission* of breaches of *the EU Regulation* and *the Transfer of Funds Ordinance*.

73. The *board* of a *PSP* must ensure that any failure by it (the *PSP*) to comply with *the EU Regulation* or *the Transfer of Funds Ordinance* is promptly reported to *the Commission*. A *PSP* must report

all material failures to comply with the *Commission Rules* in this Chapter and any serious breaches of the *PSP*'s policies, procedures and controls in respect of transfers of funds.

74. Notifications to *the Commission* should be made promptly and contain the following information:

(a) the specific provision in *the EU Regulation*, *the Transfer of Funds Ordinance*, *Commission Rules* and all of the *PSP*'s policies, procedures and controls which have been breached;
(b) the nature of the breach, including its cause;
(c) the date the breach was identified by the *PSP*; and
(d) where possible a summary of the measures taken by the *PSP* in relation to the breach and any subsequent changes to its policies, procedures and controls to mitigate against a recurrence.

75. In order to ensure that the breach is reported promptly, a *PSP* should consider filing an initial report covering items (a) to (c) in Paragraph 14.74. above, together with the steps it is considering taking under (d).

76. A *PSP* must establish policies and procedures for the internal reporting by *employees* of breaches of *the EU Regulation* or *the Transfer of Funds Ordinance*, and maintain a record of those breaches and action taken. Such policies and procedures must ensure sufficient confidentiality and protection for *employees* who report breaches committed within the *PSP*.

14.9. Record Keeping

77. Article 16 of *the EU Regulations* requires the *PSP* of the *payer* and of the *payee* to retain all records of any information received on the *payer* and *payee* of a transfer of funds for at least five years from the date of the transfer of funds.

78. Except where the relevant derogations from *the EU Regulation* apply, the *PSP* of the *payer* shall retain the following information for a period of at least five years from the date of the transfer:

(a) the name of the *payer*, the *payer's* payment *account* number and the *payer's* address, national identity number, *customer* identification number or date and place of birth; and
(b) the name of the *payee* and the *payee's* payment *account* number.

79. Except where the relevant derogations from *the EU Regulations* apply, the *PSP* of the *payee* shall retain verification information on the *payee* for a period of at least five years from the date of the transfer.

Chapter 15
Employee Screening and Training

Contents of this Chapter

15.1. Introduction

1. One of the most important tools available to the firm to assist in the prevention and detection of financial crime is to have appropriately screened *employees* who are alert to the potential *risks* of *ML*, *TF* and *PF* and who are well trained in the requirements concerning *CDD* and the identification of unusual activity, which may prove to be suspicious.

2. The effective application of even the best designed systems, policies, procedures and controls can be quickly compromised if *employees* lack competence or probity, are unaware of, or fail to apply, the appropriate policies, procedures and controls or are not adequately trained.

3. The term *employee* is defined in *Schedule 3* as any person working for the firm and includes individuals working under a contract of employment (including on a temporary basis), as well as those working under a contract for services or otherwise. This includes directors, both executive and non-executive, partners and persons employed by external parties fulfilling a function in relation to the firm under an outsourcing agreement or a contract for services.

15.2. Board Oversight

4. The *board* must be aware of the obligations of the firm in relation to *employee* screening and training.

5. The firm must ensure that the training provided to *relevant employees* is comprehensive and ongoing and that *employees* are aware of *ML*, *TF* and *PF*, the *risks* and vulnerabilities of the firm to it, and their obligations in relation to it.

6. The firm must establish and maintain mechanisms to measure the effectiveness of the AML, CFT and CPF training provided to *relevant employees*.

7. Further information on the monitoring and testing of the firm's training policies and procedures can be found within Section 2.4. of this *Handbook*.

8. In order to measure the effectiveness of AML, CFT and CPF training, the firm could consider it appropriate to incorporate an exam or some form of assessment into its on-going training programme, either as part of the periodic training provided to *relevant employees* or during the intervening period between training.

9. Regardless of the methods utilised, the *board* should ensure that it is provided with adequate information on a sufficiently regular basis in order to *satisfy* itself that the firm's *relevant employees* are suitably trained to fulfil their personal and corporate responsibilities.

10. Where the firm outsources its *MLRO* and/or *MLCO* functions to a third party, it should also consider the content of Section 2.5. of this *Handbook*, which sets out the steps the firm should take to ensure that the outsourced service provider has appropriate policies, procedures and controls surrounding the hiring and training of *employees*.

15.3. Screening Requirements

11. In accordance with Paragraph 13(1) of *Schedule 3*, the firm shall maintain appropriate and effective procedures, proportionate to the nature and size of the firm and to its *risks*, when hiring *employees* or admitting any person as a partner in the firm, for the purpose of ensuring high standards of *employee* and partner probity and competence.

12. In order to ensure that *employees* are of the required standard of competence and probity, which will depend on the role of the *employee*, the firm must give consideration to the following prior to, or at the time of, recruitment:

    (a) obtaining and confirming appropriate references;
    (b) obtaining and confirming details of any regulatory action or action by a professional body taken against the prospective *employee*;
    (c) obtaining and confirming details of any criminal convictions, including the provision of a check of the prospective *employee's* criminal record (subject to the Rehabilitation of Offenders (Bailiwick of Guernsey) Law, 2002 as amended); and
    (d) obtaining and confirming details of employment history, qualifications and professional memberships.

13. The firm must ensure that its consideration under *Commission Rule* 15.12. above, together with the results of any checks undertaken, are documented and retained.

14. In addition, the firm should give consideration to consulting the lists of specified countries and persons against whom sanctions have been imposed by the UN and the UK to ensure that a prospective *employee* does not have suspected or known involvement in terrorist activity.

15.4. Training Requirements for Relevant Employees

15. In accordance with Paragraphs 13(2) and 16A of *Schedule 3*, the firm shall ensure that *relevant employees*, and any partners in the firm, receive comprehensive ongoing training (at a frequency which has regard to the *ML*, *TF* and *PF risks* to the firm).

16. The requirements of *Schedule 3* concerning training apply to *relevant employees*, being those *employees* whose duties relate to actual *specified business* activities, including *board* members and senior management, and not necessarily to all *employees*.

17. When determining whether an *employee* is a *relevant employee* for the purposes of *Schedule 3* and this *Handbook*, the firm should take into account the following:

    (a) whether the *employee* is undertaking any *customer* facing functions or handles, or is responsible for the handling of, *business relationships* or *occasional transactions*, or transactions conducted in respect of such;
    (b) whether the *employee* is directly supporting a colleague who carries out any of the above functions;
    (c) whether an *employee* is otherwise likely to be placed in a position where they might see or hear anything which may lead to a suspicion; and
    (d) whether an *employee*'s role has changed to involve any of the functions mentioned above.

15.5. Training Requirements for Other Employees

18. There may be some *employees* who, by virtue of their function, fall outside of the definition of a *relevant employee*, for example, receptionists, filing clerks, messengers etc. The firm should consider, on a case-by-case basis, whether an *employee* falls within the definition of a *relevant employee*, as the scope of a person's role and the tasks undertaken will vary from person to person. The firm should also be aware that an *employee's* function may change over time.

19. Where the firm has concluded that an individual's role does not make them a *relevant employee*, it should be aware that those *employees* will still have obligations under *the Law*, *the Disclosure Law*, *the Terrorism Law* and other legislation. As a consequence, all *employees*, regardless of

their function, should have a basic understanding of *ML*, *TF* and *PF*, together with an awareness of the firm's internal reporting procedures and the identity of the *MLRO* and *Nominated Officer(s)*.

20. In order to achieve this the firm must as a minimum:

    (a) provide any *employee* who has not been classified as a *relevant employee* with a written explanation of the firm's and the *employee's* obligations and potential criminal liability under *the Relevant Enactments*, including the implications of failing to make an internal disclosure; and
    (b) require the *employee* to acknowledge that they understand the firm's written explanation and the procedure for making an internal disclosure.

15.6. Methods of Training

21. While there is no single or definitive way to conduct training, the critical requirement is that training is adequate and relevant to those being trained and that the content of the training reflects good practice.

22. The guiding principle of all AML, CFT and CPF training should be to encourage *relevant employees*, irrespective of their level of seniority, to understand and accept their responsibility to contribute to the protection of the firm against the *risks* of *ML*, *TF* and *PF*.

23. The precise approach adopted will depend upon the size, nature and complexity of the firm's business. Classroom training, videos and technology-based training programmes can all be used to good effect, depending on the environment and the number of *relevant employees* to be trained.

24. Training should highlight to *relevant employees* the importance of the contribution that they can individually make to the prevention and detection of *ML*, *TF* and *PF*. There is a tendency, in particular on the part of more junior *employees*, to mistakenly believe that the role they play is less pivotal than that of more senior colleagues. Such an attitude can lead to failures in the dissemination of important information because of mistaken assumptions that the information will have already been identified and dealt with by more senior colleagues.

15.7. Frequency of Training

25. The firm must provide the appropriate level of AML, CFT and CPF induction training, or a written explanation, to all new *relevant employees* or other *employees* respectively, before they become actively involved in the day-to-day operations of the firm.

26. Consideration should be given by the firm to establishing an appropriate minimum period of time by which, after the start of their employment, new *employees* should have completed their AML, CFT and CPF induction training. Satisfactory completion and understanding of any mandatory induction training should be a requirement of the successful completion of a *relevant employee's* probationary period.

27. The firm must provide AML, CFT and CPF training to all *relevant employees* at least every two years. Training will need to be more frequent to meet the requirements of *Schedule 3* if new legislation or significant changes to this *Handbook* are introduced, or where there have been significant technological developments within the firm or the introduction of new products, services or practices.

15.8. Content of Training

28. The firm must, in providing the training required pursuant to *Schedule 3* and this *Handbook*:

(a) provide appropriate training to *relevant employees* to enable them to competently analyse information and *documentation* so as to enable them to form an opinion on whether a *business relationship* or *occasional transaction* is suspicious in the circumstances;
(b) provide *relevant employees* with a *document* outlining their own obligations and potential criminal liability and those of the firm under *Schedule 3* and *the Relevant Enactments*;
(c) prepare and provide to *relevant employees* a copy, in any format, of the firm's policies, procedures and controls manual for AML, CFT and CPF; and
(d) ensure *relevant employees* are fully aware of all applicable legislative requirements.

29. In accordance with Paragraphs 13(2) and 16A of *Schedule 3*, the ongoing training provided by the firm shall cover –

(a) *the Relevant Enactments*, *Schedule 3* and this *Handbook*,
(b) the personal obligations of *employees*, and partners, and their potential criminal liability under *Schedule 3* and *the Relevant Enactments*,
(c) the implications of non-compliance by *employees*, and partners, with any rules (including *Commission Rules*), guidance, instructions, notices or other similar instruments made for the purposes of *Schedule 3*, and
(d) the firm's policies, procedures and controls for the purposes of forestalling, preventing and detecting *ML*, *TF* and *PF*.

30. In addition to the requirements of Paragraph 15.29. above, the firm must ensure that the ongoing training provided to *relevant employees* in accordance with *Schedule 3* and this *Handbook* also covers, as a minimum:

(a) the requirements for the internal and external disclosing of suspicion;
(b) the criminal and regulatory sanctions in place, both in respect of the liability of the firm and personal liability for individuals, for failing to report information in accordance with the policies, procedures and controls of the firm;
(c) the identity and responsibilities of the *MLRO*, *MLCO* and *Nominated Officer*;
(d) dealing with *business relationships* or *occasional transactions* subject to an internal disclosure, including managing the risk of tipping off and handling questions from *customers*;
(e) those aspects of the firm's business deemed to pose the greatest *ML*, *TF* and *PF risks*, together with the principal vulnerabilities of the products and services offered by the firm, including any new products, services or delivery channels and any technological developments;
(f) new developments in *ML*, *TF* and *PF*, including information on current techniques, methods, trends and typologies;
(g) the firm's policies, procedures and controls surrounding *risk* and *risk* awareness, particularly in relation to the application of *CDD* measures and the management of high *risk* and existing *business relationships*;
(h) the identification and examination of unusual transactions or activity outside of that expected for a *customer*;
(i) the nature of terrorism funding and terrorist activity in order that *employees* are alert to transactions or activity that might be terrorist-related;
(j) the vulnerabilities of the firm to financial misuse by *PEPs*, including the effective identification of *PEPs* and the understanding, assessing and handling of the potential *risks* associated with *PEPs*; and

(k) UN, UK and other sanctions and the firm's controls to identify and handle natural persons, *legal persons* and other entities subject to sanction.

31. The list included in *Commission Rule* 15.30. above is not exhaustive and there may be other areas that the firm deems it appropriate to include based on the business of the firm and the conclusions of its *business risk assessments*.

32. In accordance with Paragraph 13(3) of *Schedule 3*, the firm shall also identify *relevant employees* and partners in the firm who, in view of their particular responsibilities, should receive additional and ongoing training, appropriate to their roles, in the matters set out in Paragraph 15.29. above and it shall provide such additional training.

33. Sections 15.9. – 15.11. below set out those categories of *relevant employee* who are to be provided with additional training, together with the particular focus of the additional training provided. The categories below are not exhaustive and the firm may identify other *relevant employees* who it considers require additional training in accordance with Paragraph 15.32. above.

15.9. The Board and Senior Management

34. The *board* and senior management are responsible for ensuring that the firm has appropriate and effective policies, procedures and controls to counter the *risk* of *ML, TF* and *PF*. In accordance with Paragraph 13(3) of *Schedule 3*, the *board* and senior management must therefore be identified as *relevant employees* to whom additional training must be given in order that they remain competent to give adequate and informed consideration as to the effectiveness of those policies, procedures and controls.

35. The additional training provided to the *board* and senior management must include, at a minimum, a clear explanation and understanding of:

(a) *Schedule 3*, this *Handbook* and *the Relevant Enactments*, including information on the offences and related penalties, including potential director and shareholder liability;
(b) the conducting and recording of *ML, TF* and *PF business risk assessments* and the formulation of a *risk appetite*, together with the establishment of appropriate, relevant and effective policies, procedures and controls; and
(c) methods to assess the effectiveness of the firm's systems and controls and its compliance with *Schedule 3*, this *Handbook* and other *Relevant Enactments*.

15.10. The Money Laundering Reporting Officer and Nominated Officer

36. The *MLRO* and *Nominated Officer* are responsible for the handling of internal and external disclosures. In accordance with Paragraph 13(3) of *Schedule 3*, the *MLRO* and *Nominated Officer* must be identified as *relevant employees* to whom additional training must be given.

37. The additional training provided to the *MLRO* and *Nominated Officer* must include, at a minimum:

(a) the handling of internal disclosures of suspicious activity;
(b) the making of high quality external disclosures to the *FIU*;
(c) the handling of production and restraining orders including, but not limited to, the requirements of *the Relevant Enactments* and how to respond to court orders;
(d) liaising with *the Commission* and law enforcement agencies; and
(e) the management of the risk of tipping off.

15.11. The Money Laundering Compliance Officer

38.	The *MLCO* is responsible for monitoring and testing the effectiveness and appropriateness of the firm's policies, procedures and controls to counter the *risk* of *ML*, *TF* and *PF*. In accordance with Paragraph 13(3) of *Schedule 3*, the *MLCO* must be identified as a *relevant employee* to whom additional training must be given.

39.	The training provided to the *MLCO* must address the monitoring and testing of compliance systems and controls (including details of the firm's policies and procedures) in place to prevent and detect *ML*, *TF* and *PF*.

Chapter 16
Record Keeping

Contents of this Chapter

16.1. Introduction

1. This Chapter outlines the requirements of *Schedule 3* and the *Commission Rules* in relation to record keeping and provides guidance to the firm for the purpose of countering the threat of *ML*, *TF* and *PF*.

2. Record keeping is an essential component required by *Schedule 3* in order to assist in any financial investigation and to ensure that criminal *funds* are kept out of the financial system, or if not, that they may be detected and confiscated by the appropriate authorities. If law enforcement agencies, either in *the Bailiwick* or elsewhere, are unable to trace criminal property due to inadequate record keeping, then prosecution for *ML*, *TF* and *PF* and confiscation of criminal property may not be possible. Likewise, if the *funds* used to finance terrorist or proliferation activity cannot be traced back through the financial system, then the sources and destinations of *terrorist* or *proliferation financing* will not be identifiable.

3. Sound record keeping is also essential to facilitate effective supervision, allowing *the Commission* to supervise compliance by the firm with its statutory obligations and regulatory requirements. For the firm, sound record keeping provides evidence of the work it has undertaken to comply with those statutory obligations and regulatory requirements, as well as allowing for it to make records available on a timely basis, i.e. promptly to domestic competent authorities pursuant to *Schedule 3* or *the Relevant Enactments* and to auditors.

4. To ensure that the record keeping requirements of *Schedule 3* and this *Handbook* are met, the firm must have appropriate and effective policies, procedures and controls in place which require that records are prepared, kept for the stipulated period and in a readily retrievable form.

16.2. Relationship and Customer Records

5. In accordance with Paragraph 14(2) of *Schedule 3*, the firm shall keep:

   (a) all *transaction documents* (as detailed in Section 16.3. below), *relationship risk assessments*, and any *CDD information*, or
   (b) copies thereof,

   for the *minimum retention period*.

6. In order to meet the requirements of Paragraph 14(2) of *Schedule 3* in relation to *transaction documents*, *relationship risk assessments* and *CDD information*, the firm must keep the following records:

   (a) copies of the *identification data* obtained to verify the identity of all *customers*, *beneficial owners* and other *key principals* (for example, copies of records of official identification *documents* such as passports, identity cards, driving licences or similar);
   (b) copies of any *relationship risk assessments* carried out in accordance with Paragraph 3(4) of *Schedule 3* and Chapter 3 of *this Handbook*; and
   (c) copies of any *customer* files, *account* files, business correspondence and information relating to the *business relationship* or *occasional transaction*, including the results of any analysis undertaken (for example, inquiries to establish the background and purpose of complex, unusual or large transactions); or
   (d) information as to where copies of the *CDD information* may be obtained.

7. In accordance with Paragraph 21(1) of *Schedule 3*, the *minimum retention period* in the case of any *CDD information* is:

   (i) a period of five years starting from the date –

      (A) where the *customer* has established a *business relationship* with the firm, that relationship ceased,
      (B) where the *customer* has carried out an *occasional transaction* with the firm, that transaction was completed, or

   (ii) such other longer period as *the Commission* may direct.

16.3. Transaction Records

8. In accordance with Paragraph 14(1) of *Schedule 3*, the firm shall keep a comprehensive record of each transaction with a *customer* or an *introducer*, including the amounts and types of currency involved in the transaction (if any); and such a record shall be referred to as a "*transaction document*".

9. In order to meet the requirements of Paragraph 14(1) of *Schedule 3* to keep each *transaction document*, all transactions carried out on behalf of or with a *customer* in the course of business, both domestic and international, must be recorded by the firm. In every case sufficient information must be recorded to permit the reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

10. The firm must ensure that, in order to meet the record keeping requirements for a transaction, *documentation* is maintained which must include:

   (a) the name and address of the *customer* and *beneficial owner*;
   (b) for a monetary transaction, the amounts and types of currency involved in the transaction;
   (c) the *account* name and number or other information by which it can be identified;
   (d) details of the counterparty, including *account* details;
   (e) the nature of the transaction; and
   (f) the date of the transaction.

11. Records relating to unusual and complex transactions and high *risk* transactions must include the firm's own reviews of such transactions.

12. In accordance with Paragraph 21(1) of *Schedule 3*, the *minimum retention period* is, in the case of any *transaction document* –

   (i) a period of five years starting from the date that the transaction and any related transaction were completed, or
   (ii) such other longer period as *the Commission* may direct.

13. In accordance with Paragraph 14(4) of *Schedule 3*, where the firm is required by any enactment, rule of law or court order to provide a *transaction document* or any *CDD information* to any person before the end of the minimum retention period, the firm shall –

   (a) keep a copy of the *transaction document* or *CDD information* until the period has ended or the original is returned, whichever occurs first, and
   (b) maintain a register of *transaction documents* and *CDD information* so provided.

16.4. Wire Transfers

14. Section 7 of the *Transfer of Funds Ordinance* requires the *PSP* of the *payee* to retain all records of any information received on the *payer* of a transfer of *funds* for five years from the date of the transfer of *funds*.

16.5. Internal and External Disclosures

15. In accordance with Paragraph 14(5)(a) of *Schedule 3*, the firm shall keep records of any internal disclosures made to the *MLRO* or a *Nominated Officer* and of any external disclosures made under Part I of *the Disclosure Law* or Section 15 or 15A, or Section 12 (as appropriate), of *the Terrorism Law* made other than by way of an internal disclosure to the *MLRO*.

16. In meeting the requirements of Paragraph 14(5)(a) of *Schedule 3* related to disclosures, the firm must keep:

(a) the internal disclosure and any supporting *documents*;
(b) records of actions taken under the internal and external reporting requirements;
(c) evidence of the enquiries made in relation to that internal disclosure;
(d) where the *MLRO* (or a *Nominated Officer*) has considered information or other material concerning possible *ML, TF* and *PF*, but has not made an external disclosure to the *FIU*, a record of the other material that was considered and the reason for the decision; and
(e) where an external disclosure has been made to the *FIU*, evidence of the *MLRO's* (or *Nominated Officer's*) decision and copies of all relevant information passed to the *FIU*.

17. In addition to the above, the firm must maintain a register covering both internal disclosures and external disclosures made to the *FIU*, and include the following as a minimum:

(a) the date the internal disclosure was received by the *MLRO* (or the *Nominated Officer*);
(b) the name of the person submitting the internal disclosure;
(c) the date of the disclosure to the *FIU* (if applicable);
(d) the name of the person who submitted the disclosure to the *FIU* (if applicable);
(e) the value of the transaction or activity subject to the disclosure (where available);
(f) a reference by which supporting evidence is identifiable; and
(g) the date(s) of any update(s) (additional information) submitted to the *FIU*.

18. In accordance with Paragraph 14(5)(a)(i)-(iii) of *Schedule 3*, the *minimum retention period* for disclosures is five years starting from –

(a) in the case of an internal or external disclosure in relation to a *business relationship*, the date the *business relationship* ceased,
(b) in the case of an internal or external disclosure in relation to an *occasional transaction*, the date that the transaction was completed, or
(c) in any other case, the event in respect of which the internal or external disclosure was made.

16.6. Training Records

19. In accordance with Paragraph 14(5)(b) of *Schedule 3*, the firm shall keep records of any training carried out under Paragraph 13 of *Schedule 3* for five years starting from the date the training was carried out.

20. In order to meet the requirements of Paragraph 14(5)(b) of *Schedule 3* to keep records of AML, CFT and CPF training undertaken, the firm must record the following as a minimum:

(a) the dates training was provided;
(b) the nature of the training; and
(c) the names of the *employees* who received the training.

16.7. Business Risk Assessments

21. In accordance with Paragraph 14(3) of *Schedule 3*, the firm shall keep copies of *business risk assessments* carried out under Paragraph 3(1) of *Schedule 3* until the expiry of the period of five years starting from the date on which they cease to be operative.

16.8. Policies, Procedures, Controls and Compliance Monitoring

22. In accordance with Paragraph 14(5)(c)-(d) of *Schedule 3*, the firm shall keep any minutes or other *documents* prepared pursuant to Paragraph 15(1)(c) of *Schedule 3*, until –

(i) the expiry of a period of five years starting from the date they were finalised, or
(ii) they are superseded by later minutes or other *documents* prepared under that paragraph,

whichever occurs later, and its policies, procedures and controls which it is required to establish and maintain pursuant to *Schedule 3*, until the expiry of a period of five years starting from the date that they ceased to be operative.

23. In order to meet the requirements Paragraph 14(5)(c)-(d) of *Schedule 3*, the firm must retain:

(a) reports made by the *MLRO* and *MLCO* to the *board* and senior management;
(b) records or minutes of the *board's* consideration of those reports and of any action taken as a consequence; and
(c) any records made within the firm or by other parties in respect of the firm's compliance with *Schedule 3* and this *Handbook*.

16.9. Closure or Transfer of Business

24. Where the firm terminates activities or disposes of a business or a block of *business relationships* (for example, by way of asset sale to another firm) the person taking on that business must ensure that the record keeping requirements of *Schedule 3* and this *Handbook* are complied with in respect of such business.

16.10. Ready Retrieval

25. In accordance with Paragraph 14(6) of *Schedule 3*, *document*s and *CDD information*, including any copies thereof, kept in accordance with *Schedule 3*, may be kept in any manner or form, provided they are readily retrievable.

26. Periodically the firm must review the ease of retrieval, and condition, of paper and electronically retrievable records.

27. In accordance with Paragraph 14(6)(b) of *Schedule 3*, *documents* and *CDD information*, including any copies thereof, kept in accordance with *Schedule 3*, shall be made available promptly:

(i) to an auditor; and

(ii) to any *police officer*, the *FIU*, *the Commission* or any other person, where such *documents* or *CDD information* are requested pursuant to *Schedule 3* or any of *the Relevant Enactments*.

28. The firm must consider the implications for meeting the requirements of *Schedule 3* where *documentation*, data and information is held overseas or by third parties, such as under outsourcing arrangements, or where reliance is placed upon an *introducer*.

29. The firm must not enter into outsourcing arrangements or place reliance on third parties to retain records where access to those records is likely to be restricted.

30. Where the *FIU* or another domestic competent authority requires sight of records, either under *Schedule 3* or another of *the Relevant Enactments*, which according to the applicable procedures would ordinarily have been destroyed, the firm must nonetheless conduct a search for those records and provide as much detail to the *FIU* or other domestic competent authority as possible.

16.11. Manner of Storage

31. The record keeping requirements are the same regardless of the format in which the records are kept, or whether the transaction was undertaken by paper or electronic means.

32. Records may be retained:

(a) by way of original *documents*;
(b) by way of photocopies of original *documents* (certified where appropriate);
(c) on microfiche;
(d) in a scanned form; or
(e) in a computer or electronic form (including cloud storage).

33. The use of technology to collect and/or store data and *documents* does not alter the obligations and requirements described in this *Handbook*.

34. Where the firm utilises an electronic method of gathering *identification data*, for example, an App. or other system as set out in Section 5.6. of this *Handbook* or a *CDD* Utility, the firm should include within its *risk* assessment of that technology an evaluation of the policy for the retention of *document*s. This evaluation should enable the firm to ensure that its use of the technology complies with the requirements of *Schedule 3* and this *Handbook* and that the firm will not incur legal evidential difficulties (for example, in civil court proceedings).

Chapter 17
Transitional Provisions

Contents of this Chapter

17.1. Introduction

1. This Chapter details the measures to be implemented by the firm in order to transition existing compliance arrangements under the Criminal Justice (Proceeds of Crime) (Financial Services Business) (Bailiwick of Guernsey) Regulations, 2007 as amended ("*the FSB Regulations*") and/or the Criminal Justice (Proceeds of Crime) (Legal Professionals, Accountants and Estate Agents) (Bailiwick of Guernsey) Regulations, 2008 as amended ("*the PB Regulations*") to the requirements of *Schedule 3* and the *Commission Rules* set out in this *Handbook*. This Chapter also provides the deadlines by which such revised controls are required to be implemented.

2. In accordance with Paragraph 4(1) of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) Ordinance, 2018 ("*the Amendment Ordinance*"), the requirements of *Schedule 3* shall come in to force on 31 March 2019.

3. In order to assist the firm in transitioning to the new regime, a tiered approach to the review of existing *business relationships* has been provided, allowing the firm to update its *relationship risk assessments* and *CDD information* as part of its regular monitoring and ongoing *CDD* arrangements.

4. This Chapter covers the particular aspects of *Schedule 3* and the *Commission Rules* where material changes have been made to the requirements of the previous regime. There may be other changes required which are not covered in this Chapter. The firm should therefore have regard to the content of *Schedule 3* and this *Handbook* in their entirety when considering the full scope of the changes required to be made.

17.2. Business Risk Assessments

5. As identified in Chapter 3 of this *Handbook*, a *risk*-based approach starts with the identification and assessment of the *risk* that has to be mitigated and managed. Consideration of the information obtained as part of the firm's *ML, TF* and *PF business risk assessments* will enable the firm to assess the appropriate controls required to mitigate and manage any *risks* arising.

6. In accordance with Paragraphs 3(1), 3(8) and 16A (4) of *Schedule 3*, the firm shall carry out and document a suitable and sufficient *ML business risk assessment*, a suitable and sufficient *TF business risk assessment*, as soon as reasonably practicable after 31 March 2019, and a suitable and sufficient *PF business risk assessment*, as soon as reasonably practicable after 29 February 2024 which are specific to the firm, (and this shall be construed consistently with the provisions of this *Handbook*).

7. In order to meet the requirements of Paragraph 3 of *Schedule 3* and Chapter 3 of this *Handbook*, the firm must review its existing *business risk assessment* to ensure that it contains suitable, sufficient and separate assessments of the *ML, TF* and *PF risks* to the firm.

8. For the purposes of Paragraph 17.6. above:

   (a) the firm must have reviewed its *business risk assessment* and have had the revised *ML* and *TF* assessments approved by the *board* of the firm by no later than 30 September 2020;
   (b) the firm must have reviewed its *business risk assessment* and have had the revised PF assessment approved by the *board* of the firm by no later than 31 December 2024; and
   (c) the conclusions of *the Bailiwick's NRA* must be taken into account as part of the next review of the *business risk assessment* as required by Paragraph 3(1) of *Schedule 3*.

17.3. Policies, Procedures and Controls

9. As part of a *risk*-based approach, the policies, procedures and controls devised and utilised by the firm will be determined by its assessment of the *risks* of *ML*, *TF* and *PF* to its business. In this regard, the policies, procedures and controls of the firm should be reviewed in parallel with the *business risk assessments* to ensure that any changes in the perceived threats and vulnerabilities of the firm are mitigated and managed by its controls.

10. In accordance with Paragraphs 3(6) and 3(8) of *Schedule 3*, the firm shall review its policies, procedures and controls as soon as reasonably practicable after 31 March 2019 to ensure that they remain appropriate and effective, in light of both the revisions to the *business risk assessments* of the firm in accordance with Paragraph 17.6. above and the requirements of *Schedule 3*, this *Handbook* and the *risks* relevant, or potentially relevant, to the firm identified in the *NRA*.

11. For the purposes of Paragraph 17.10.:

(a) the firm must have reviewed and revised its policies, procedures and controls, and these must have been approved by the *board*, by no later than 30 September 2020; and
(b) the conclusions of the *Bailiwick's NRA* must be taken into account as part of the next review of the firm's policies, procedures and controls as required by Paragraph 3(6) of *Schedule 3*.

12. In reviewing its policies, procedures and controls, the firm should seek to ensure that they appropriately mitigate any *risks* arising from the revised *business risk assessments*. Examples include, but are not limited to:

(a) *customer* take-on procedures: to ensure that any changes required to the *relationship risk-assessment* process are taken into account, together with any changes to the *CDD* and *CDD information* required for various types of *customer*;
(b) *employee* training arrangements: to ensure that any new or amended *risks* identified as part of the revised *business risk assessment* are communicated to *employees*, together with the firm's *risk appetite* and tolerance; and
(c) any automated screening/monitoring tools used to identify *PEPs*: to ensure that *domestic PEPs* and *international organisation PEPs* are flagged as appropriate.

13. In accordance with Paragraph 3(9) of *Schedule 3*, without prejudice to Paragraph 17.10. above, until the firm has complied with Paragraph 3(6)(a) of *Schedule 3*, it shall continue to maintain the policies, procedures and controls it was required to establish and maintain under *the FSB Regulations* and/or *the PB Regulations*.

17.4. Money Laundering Reporting Officer

14. In accordance with Paragraph 12(1)(a) of *Schedule 3*, the firm shall appoint a person of at least management level as the *MLRO*, provide the name, title and email address of that person to *the Commission* as soon as is reasonably practicable and, in any event, within fourteen days starting from the date of that person's appointment, and ensure that all *employees* are aware of the name of that person.

15. Paragraph 12(2) of *Schedule 3* provides that a person who, immediately prior to the coming into force of *Schedule 3*, was the *MLRO* of the firm, having been appointed as such under Part III of *the FSB Regulations* or Part III of *the PB Regulation*, as the case may be, shall be deemed to have been appointed as the *MLRO* under Paragraph 12(1)(a) of *Schedule 3* as at the date that *Schedule 3* comes into force. Accordingly, Paragraph 12(4) of *Schedule 3* affirms that the requirement to *notify the Commission* and the *FIU* of the name, title and email address of the *MLRO* does not apply to any such persons.

16. Where the firm's *MLRO* appointed under *the FSB Regulations* and/or *the PB Regulations* will not take such an appointment under *Schedule 3*, the firm must ensure that *the Commission* and the *FIU* are *notified* by 14 April 2019.

17. Notification of any changes to the *MLRO* should be made via *the Commission's* Online PQ Portal.

https://online.gfsc.gg

17.5. Money Laundering Compliance Officer

18. In accordance with Paragraph 15(1)(a) of *Schedule 3*, the firm shall, if it comprises more than one individual, appoint a person of at least management level as the *MLCO* and provide the name, title and email address of that person to *the Commission* as soon as is reasonably practicable and, in any event, within fourteen days starting from the date of that person's appointment.

19. Further information on the role of the *MLCO*, including the requirements in respect of the individual appointed, can be found in Section 2.8.1. of this *Handbook*.

20. The *board* of the firm must ensure that a suitable *MLCO* is appointed by 31 March 2019 and *the Commission* must be *notified* by 14 April 2019 of that person's appointment

21. Notification of an individual's appointment as *MLCO* should be made via *the Commission's* Online PQ Portal.

22. For the avoidance of doubt, in accordance with Paragraph 2.78. of this *Handbook*, the natural person who holds the role of *MLRO* can also be appointed as the firm's *MLCO*.

17.6. Existing Business Relationships

23. In accordance with Paragraph 4(1)(b) of *Schedule 3*, the firm shall ensure that the *CDD* measures set out at Paragraph 4(3) of *Schedule 3* are applied to all *business relationships* established prior to the coming in to force of *Schedule 3* –

    (a) in respect of which there is maintained an anonymous *account* or an *account* in a fictitious name, as soon as possible after the coming in to force of *Schedule 3* and in any event before such *account* is used again in any way, and
    (b) where it does not fall within (a) and to the extent that such steps have not already been carried out, at appropriate times on a *risk*-sensitive basis.

24. Additionally, in accordance with Paragraph 8(1)(b) of *Schedule 3*, the firm shall, in relation to all *customers*, maintain *accounts* in a manner which facilitates the meeting of the requirements of *Schedule 3*, and the relevant *Commission Rules* and *guidance* in this *Handbook*.

25. The firm should apply the *relationship risk assessment* and *CDD* requirements of *Schedule 3* and this *Handbook*, including the application of *enhanced measures* as necessary, to existing *business relationships* at appropriate times on the basis of materiality and *risk*. This provides for the firm to apply the requirements of *Schedule 3* and the *Commission Rules* sensibly and to consider all relevant factors rather than carrying out a 'tick box' exercise.

26. The review of *relationship risk assessments* and *CDD information*, and the application of *CDD* and *enhanced measures* in accordance with *Schedule 3* and this *Handbook*, should be conducted at appropriate times, taking into account whether and when any *CDD* measures have previously been applied and the adequacy of the *identification data* held. Whilst *Commission Rules* 17.27.

and 17.28. below, enable the firm to determine how best to manage the review within the timeframe set, *the Commission* would encourage the firm to take a *risk* based approach to ensure that current *CDD* measures, including *ECDD* and/or *enhanced measures* where relevant, are applied to its high *risk business relationships* well in advance of 31 December 2021. Setting a 30 June 2021 deadline for reviewing all high *risk business relationships* would be prudent.

27. Notwithstanding the above, the *board* must ensure that **all** *business relationships* are reviewed by 31 December 2021.

28. In complying with Paragraph 8 of *Schedule 3*, as part of the reviews conducted by the firm in accordance with *Commission Rule* 17.27. above, the firm must take all steps deemed necessary to ensure that *relationship risk assessments* are conducted and appropriate *CDD* measures applied, including *ECDD* and/or *enhanced measures* where relevant, in accordance with Paragraphs 2 to 8 of *Schedule 3* and Chapters 3 to 9 of this *Handbook*.

29. Where, following a review, the firm has concluded that the overall *risk* of a *business relationship* has not changed and it considers that the *CDD information* held appropriately verifies the identity of, and mitigates the specific *risks* associated with, that *customer* (and the *beneficial owner* and any other *key principals* thereof), in accordance with Paragraph 11.43. of this *Handbook* the firm is not required to re-verify the identity of the *customer*, *beneficial owner* and other *key principals*.

30. When determining whether it is necessary to gather additional *CDD information*, the firm should review and research whether existing records contain the required items. The firm may have had a *business relationship* for many years and therefore already hold considerable information concerning the *customer*. In these circumstances research should be undertaken to clarify whether it is a matter of collating records before further approaching a *customer* or other *key principal*.

31. Where the firm has concluded that the *CDD information* held is not sufficient to enable compliance with *Schedule 3* and the *Commission Rules*, prior to reverting to a *customer* or other *key principal* the firm should consider the materiality of the extra information/documentation required and whether compliance could be achieved through alternate means. Such alternate means could be through the use of online databases or verification tools to provide additional *identification data*, or corroborate any *identification data* held.

32. Where the firm holds certified *identification data* which was obtained prior to the coming in to force of *Schedule 3* and this *Handbook*, provided the firm is satisfied as to the veracity of the *identification data* held and the certification provided in connection with that *identification data*, the firm is not required to re-certify (or seek newly certified) *identification data*.

17.7. Collective Investment Schemes – Nominated Firm for Investor CDD

33. In accordance with Paragraph 4.59. of this *Handbook*, each CIS authorised or registered by *the Commission* must nominate a firm licensed under *the POI Law* to be responsible for the application of *CDD* measures to all investors in that CIS.

34. As required by *Commission Rule* 4.61., the nominated firm must treat the investors into the CIS for which it has been nominated as if they were its *customers* and deal with them in accordance with the requirements of *Schedule 3* and this *Handbook*.

35. Where a CIS already holds an authorisation or registration issued by *the Commission*, the nominated firm must *notify the Commission* by the 31 May 2019 that it has been so nominated.

36. As an initial means of *notifying the Commission* of the firm's nomination by a CIS in accordance with *Commission Rule* 17.35. above, a one-off form entitled 'Notification of the Firm's

Nomination for Investor CDD' will be made available via *the Commission's* Online Submissions Portal for all firms licensed under *the POI Law*.

https://submit.gfsc.gg/

Chapter 18
Virtual Assets

Contents of this Chapter

18.1. Introduction

1. The purpose of this Chapter is to provide Virtual Asset Service Providers ("*VASP*s") with guidance on how to meet their obligations within *Schedule 3* and the rules of this *Handbook*, and it contains rules and guidance on the information required to accompany *transfers* of *virtual assets*. The guidance in this Chapter is in addition to, and not in place of, the guidance within other chapters of this *Handbook*. *VASP*s fall within the definition of a *specified business* and therefore the *Handbook* is applicable to such firms.

2. The Lending, Credit and Finance (Bailiwick of Guernsey) Law, 2022 was brought into full effect on 1 July 2023 and introduced regulation of *VASP*s to bring *the Bailiwick* in line with international standards, issued by FATF.

3. This Chapter also provides guidance for specified business which are not licensed as *VASP*s but have *business relationships* or *occasional transactions* with a connection to, or involvement with, *virtual assets* ("*VA*s") – examples where this may arise include where a *customer*'s source of wealth or funds derives from *virtual assets*, or an investment within a structure administered by a *specified business* holds *virtual assets*.

4. *VASP*s are firms which provide or carry out exchange, *transfer*, safe-keeping, administration, custody, issue, offer, sale, distribution, trading and other activities in connection with *virtual assets* from *the Bailiwick*. *VASP*s are required to hold a Part III *VASP* licence under *the LCF Law*.

5. *The LCF Law* does not seek to regulate the technology underlying *VA*s or *VASP*s, but rather the natural or *legal person* or *legal arrangement* that may use the technology or software applications to conduct *virtual asset* services as a business.

18.2. Risk-Based Approach

6. The *virtual asset* sector is global and the *ML*, *TF* and *PF* risks facing each business will vary depending on the type of products offered, the *customers* and the delivery channels. The cross-border nature of, potential enhanced-anonymity associated with, and non-face-to-face *business relationships* and transactions facilitated by *virtual asset* activities (whether licensed or not) could indicate higher risks of *ML*, *TF* and *PF*, therefore *VASP*s should have appropriate policies, procedures and controls to identify, understand, assess and mitigate these *risks* where applicable.

7. Section 10.2(2) of the Lending, Credit and Finance Rules and Guidance, 2023 prohibits Part III *VASP* licensees from dealing in, trading in, or offering *virtual assets* or *virtual asset* services which aim to obscure either the parties to the transaction or the flow of the assets, *VASP*s should therefore consider how they will demonstrate that this is adhered to. For example, *VASP*s should consider whether technological methods have been used to further obfuscate the traceability of *VA* transactions and whether there is technology available to detect such obfuscation.

8. Managing the cybercrime risks and activities to which *VASP*s are susceptible is important and requires the *VASP* to assess and mitigate the cyber risks it faces by establishing appropriate controls to reduce these risks. As *VASP*s are regulated under *the Regulatory Laws*, they must comply with the Cyber Security Rules and Guidance 2021.

9. Example risk factors specific to *virtual assets* are included at the end of this Chapter and should be considered by *VASP*s and *specified businesses* involved with *virtual asset* activities.

18.3 Customer Due Diligence

10. The earlier Chapters in this *Handbook* set forth the required *CDD* measures that *specified businesses* must apply to *business relationships* and *occasional transactions*. These will also apply to *VASP*s. This includes *CDD* measures and where relevant in accordance with Chapter 8 *enhanced measures* and *ECDD*. One notable exception is that, per *Schedule 3* to *the Law*, the designated threshold above which *CDD* must be conducted for an *occasional transaction* in respect of *VASP*s is lower and relates to any transaction or linked transactions involving more than £1,000.

11. Upon establishing *VASP* operating policies, procedures and controls when accepting *customers* and facilitating transactions, *VASP*s should consider how they will determine if it's a *business relationship* or an *occasional transaction*. It should ensure that an *occasional transaction* is conducted on a one-off or occasional basis, rather than on a more consistent basis. Where a *customer* opens an account with the *VASP*, where an element of duration is likely, it should be considered a *business relationship*.

12. *VASP*s are encouraged to collect additional information to assist them in verifying the *customer*'s identity when establishing a *business relationship* or carrying out an *occasional transaction*; to authenticate the identity of *customers* for account access; to help determine the *customer*'s business and risk profile and conduct ongoing due diligence on the *business relationship*; and mitigate the *ML, TF* and *PF risks* associated with the *customer* and the *customer*'s financial activities. Such additional information could include, for example, an IP address with an associated time stamp, geo-location data, device identifiers, *virtual asset* wallet addresses and/or transaction hashes. In addition, *VASP*s should also understand whether a *customer*'s virtual wallet address relates to a private wallet, a multi-signature wallet or a custodial wallet.

13. Whilst *VASP*s are required to build a *risk* profile of their *customers*, they should also consider whether a *risk* profile of a cluster of *customers* displaying homogenous characteristics (for example, *customers* conducting similar types of *virtual asset* transactions or involving the same *virtual asset*) would be beneficial, for example, to make monitoring via appropriate parameters on monitoring systems easier. Where a cluster of *customers* is identified, the *VASP* should clearly document the criteria and parameters used to allocate *customers* to a cluster.

14. As part of a *VASP*'s ongoing monitoring, it should screen its *customers*' and counterparties' wallet addresses against available blacklisted wallet addresses, adverse media and sanctions and determine whether mitigation or preventive actions are warranted in the event of a positive hit. Where available, *VASP*s should use analytical tools available to them to detect potentially fraudulent transactions and other suspicious activity, for example, that the *VA*s were used on the dark web or in connection with a ransomware attack. Where this is not possible this should increase the *risk* profile of the *customer*.

15. Where a *VASP* is undertaking source of wealth verification and where the source of wealth disclosed is from mining or staking *virtual assets*, documentation on the mining operation could be through the collection of electricity bills and hardware receipts etc. and an assessment should be made as to whether the *customer* can afford to run the mining operation given their declared source of wealth. Documentation on the staking could be via the smart contract entered into for the staking, or through analysis of the *customer*'s blockchain address. Where money has been paid out from a mining or staking pool, the *VASP* should obtain evidence that the address from which the *VA*s were transferred is controlled by a mining or staking pool and that the *customer* had a connection with the mining or staking pool.

16. Where funds are being returned due to insufficient *CDD*, they must be returned to the same account they were paid from and should be accompanied with script stating they are being refunded due to the inability to complete *CDD*. Where this is the case, consideration should be given to making a disclosure to the *FIU* in accordance with Chapter 13 on reporting suspicion.

17. When transaction information is easily available on a public ledger or via other open sources, *VASP*s must still record and retain that information in accordance with Chapter 11 on monitoring transactions and activity.

18.4. Enhanced Customer Due Diligence

18. There are *ECDD* measures which can be undertaken in relation to *VA*s in addition to those already included within Chapter 8 on *enhanced customer due diligence*. Examples of additional steps the firm could take when meeting the requirements of Paragraphs5(3)(v)(A)-(D) of *Schedule 3* while undertaking *ECDD* in relation to *VA*s could include, but is not limited to, applying one or more of the following measures most relevant towards mitigating the *ML, TF* and/or *PF* risks:

    (a) corroborating the identity information received from the *customer*, such as a national identity number, with information in third-party databases or other reliable sources;
    (b) tracing the *customer*'s IP address;
    (c) using blockchain analysis products, or other suitable services, from a reliable commercial vendor;
    (d) using open source to corroborate activity information consistent with the *customer*'s transaction profile; and/or
    (e) collecting additional information on:
        i. the purpose of the transaction or payment;
        ii. details about the nature, end use or end user of the item;
        iii. proof of funds ownership;
        iv. parties to the transaction and the relationship between the parties;
        v. the identity and beneficial ownership of the counterparty; and
        vi. export control information, such as copies of export control or other licenses issued by a national export control authority, and end user certification.

18.5. Correspondent Banking and Other Similar Relationships

19. Correspondent banking (the provision of banking services by one *bank* to another *bank*) and other similar relationships do not include one-off transactions, but instead are characterised by their ongoing, repetitive nature. *VASP*s should define and assess the characteristics of their counterparty *VASP* relationships and ascertain whether they are undertaking activities similar to correspondent banking. Where it is established that a *VASP* is entering into a relationship that is similar to correspondent banking, it should adhere to the rules and guidance included within Section 8.6 of this *Handbook* on correspondent banking.

18.6. *Transfers*

20. *VASP*s are required to obtain, hold and submit required *originator* and beneficiary information associated with the *transfers* of *virtual assets* in order to identify and report suspicious transactions, take freezing actions and prohibit transactions with designated persons and entities. This is similar to the *wire transfer* requirements included within Chapter 14.

21. *The Commission* does not require a particular technology or software to be used to comply with the *transfer* rules. Any technology or software used must enable the *originator* and *beneficiary VASP*s to comply with their AML/CFT/CPF obligations.

22. The technology or software used should enable *VASP*s to comply with the *transfer* rules in an effective and efficient manner and enable *VASP*s to undertake the following actions:

    a) Enable a *VASP* to locate counterparty *VASP*s for *transfers* of virtual assets;

b) Enable the submission of required and accurate *originator* and required beneficiary information immediately when a *virtual asset transfer* is conducted on a distributed ledger technology platform;
c) Enable *VASP*s to submit reasonably large volume of transactions to multiple destinations in an effectively stable manner;
d) Enable a *VASP* to securely transmit data, i.e., protect the integrity and availability of the required information to facilitate record-keeping;
e) Protect the use of such information by receiving *VASP*s or other entities involved with *virtual assets* as well as to protect it from unauthorised disclosure in line with Guernsey data protection legislation;
f) Provide a *VASP* with a communication channel to support further follow-up with a counterparty *VASP* for the purpose of:

(i) Due diligence on the counterparty *VASP*; and
(ii) Requesting information on a certain transaction to determine if the transaction involved high risk or prohibited activities.

18.6.1 *Transfers* of *virtual assets* to a beneficiary – *Originating VASP* obligations

23. In accordance with Paragraph 15C(1) of *Schedule 3*, in respect of any *virtual asset transfer*, an *originating VASP* shall –

(a) obtain and hold required and accurate *originator* information and required beneficiary information,
(b) ensure that the information specified in (a) accompanies the *transfer* of the *virtual asset* to the *beneficiary VASP* immediately and securely,
(c) make the information specified in (a) available on request to *the Commission* and other appropriate authorities as soon as is reasonably practicable,
(d) not execute any *virtual asset transfer* in respect of which (b) is not complied with, and
(e) in the case of a transaction which would be an *occasional transaction* but for the sum involved being under £1,000, obtain and hold such information, or information of such class or description, as may be specified for the purposes of this Part of this Schedule in requirements set out in *the Handbook*.

24. When conducting a *VA transfer*, the *originating VASP* must ensure that *VA transfers* are accompanied by the following *originator* information:

(a) the name of the *originator*;
(b) where a *transfer* of *VA*s is registered on a network using distributed ledger technology or similar technology, the *originator*'s distributed ledger address and the *originator*'s *VA* account number, where such an account exists and is used to process the transaction;
(c) where a *transfer* of *VA*s is not registered on a network using distributed ledger technology or similar technology, the *originator*'s account numbers;
(d) where a *transfer* of *VA*s is neither registered on a network using distributed ledger technology or similar technology nor is made from or to a *VA* account, the *originating VASP* shall ensure that the *transfer* of *VA*s is accompanied by a unique transaction identifier which permits traceability of the transaction;
(e) one of either:
  (i) the *originator*'s address, including the name of the country,
  (ii) national identity number,
  (iii) *customer* identification number or
  (iv) date and place of birth; and
(f) subject to the existence of the necessary field in the relevant message format, and where provided by the *originator* to the *originator*'s *VASP*, the current Legal Entity Identifier ("LEI") of the *originator* or any other available equivalent official identifier.

25. Where the *originator* is an existing *customer* of the *VASP* to whom it should have applied due diligence measures consistent with this *Handbook*, the *VASP* may deem verification to have taken place if it is appropriate to do so taking into account the risk of *ML*, *TF* and *PF*.

26. A national identity number should be any government issued personal identification number or other government issued *unique identifier*. Examples of such would include a passport number, national identity card number or social security number.

27. A *customer* identification number may be an internal reference number that is created by a *VASP* which uniquely identifies a *customer* (rather than an *account* that is operated for an *originator* or a transaction) and which will continue throughout a *business relationship*, or it may be a number that is contained within an official document.

28. Prior to conducting the *VA transfer*, the *originating VASP* must verify the accuracy of the information obtained in Commission Rule 18.24(a), (e) and (f) using documents, data or information obtained from a reliable and independent source.

29. When conducting a *VA transfer*, the *originating VASP* must ensure that *VA transfers* are accompanied by the following beneficiary information:

    (a) the name of the beneficiary;
    (b) where a *transfer* of *VA*s is registered on a network using distributed ledger technology or similar technology, the beneficiary's distributed ledger address and the beneficiary's *VA* account number, where such an account exists and is used to process the transaction;
    (c) where a *transfer* of *VA*s is not registered on a network using distributed ledger technology or similar technology, the beneficiary's account numbers;
    (d) where an account is not used to process the *transfer*, the unique transaction identifier which permits the traceability of the transaction; and
    (e) subject to the existence of the necessary field in the relevant message format, and where provided by the *originator* to the *originator*'s *VASP*, the current LEI of the *originator* or any other available equivalent official identifier.

30. The information referred to in Commission Rules 18.24 and 18.29 should be submitted in advance of, or simultaneously or concurrently with, the *transfer* of *VA*s and in a secure manner that complies with *the Data Protection Law*. It does not have to be attached directly to, or be included in, the *transfer* of *VA*s.

31. Where a *VA transfer* is made to a self-hosted address, the *originating VASP* must obtain and hold information referred to in Commission Rules 18.24 and 18.29 and ensure that the *VA transfer* can be individually identified.

32. Where a *VA transfer* of £1,000 or more is made to a self-hosted address, the *originating VASP* must take adequate measures to assess if such address is owned or controlled by the *originator*.

33. An *originating VASP* must not execute a *transfer* where it is unable to collect and maintain the required information referred to in Commission Rules 18.24 and 18.29.

34. Where a *transfer* is carried out which is under the £1,000 threshold, the *originating VASP* must obtain and hold:

    a) the name of the *originator* and the beneficiary; and
    b) the *VA* wallet address for each or a unique transaction reference number,

but it is not necessary to verify the *customer* information on the *originator* unless the *virtual assets* to be transferred have been received anonymously, or the *VASP* has reasonable grounds for suspecting *ML*, *TF* and/or *PF*.

18.6.2 *Batch Transfers*

35. In accordance with Paragraph 15E of *Schedule 3*, in the case of a *batch transfer*, an *originating VASP* shall –

    (a) ensure that the batch file contains required and accurate *originator* information and required beneficiary information,
    (b) ensure that the information specified in (a) is such as to permit the traceability within the beneficiary jurisdiction of each transaction comprised in the batch from the *originator* to the beneficiary (and "beneficiary jurisdiction" means the jurisdiction in which the *beneficiary VASP* received the *transfer* of the *virtual assets*), and,
    (c) include the *originator*'s account number or unique transaction identifier and/or such other information, or information of such a class or description, as may be specified in *the Handbook*.

36. The batch file information requirements which apply where several individual *VA transfers* with a single *originator* are bundled together for transmission in a *batch transfer* include:

    (a) the name of the *originator*;
    (b) where an account is used to process the *transfer* of *VA*s by the *originator*, the account number of the *originator*;
    (c) one of either
        (i) the *originator*'s address, including the name of the country,
        (ii) national identity number,
        (iii) *customer* identification number or
        (iv) date and place of birth;
    (d) the individual *transfers* of *VA*s carry the account number of the *originator* or a unique identifier; and
    (e) the name, account number or unique identifier of the beneficiary that is traceable in the beneficiary country.

37. Where a *batch transfer* is carried out which is under the £1,000 threshold, the *originating VASP* must obtain and hold:

    a) the name of the *originator* and the beneficiary; and
    b) the *VA* wallet address for each or a unique transaction reference number,

    but it is not necessary to verify the *customer* information on the *originator* unless the *virtual assets* to be transferred have been received anonymously, or the *VASP* has reasonable grounds for suspecting *ML*, *TF* and/or *PF*.

18.6.3 *Transfers* of *virtual assets* to a beneficiary – *Beneficiary VASP* obligations

38. In accordance with Paragraph 15C(2) of *Schedule 3*, in respect of any *virtual asset transfer*, a *beneficiary VASP* shall –

    (a) obtain and hold required and accurate beneficiary information and required *originator* information,
    (b) make the information specified in (a) available on request to *the Commission* and other appropriate authorities as soon as is reasonably practicable,

in the case of a transaction which would be an occasional transaction but for the sum involved being under £1,000, obtain and hold such information, or information of such class or description, as may be specified for the purposes of this Part of this Schedule in requirements set out in *the Handbook*.

39. On receipt of a *VA transfer*, the *beneficiary VASP* must ensure that *VA transfers* are accompanied by the following *originator* and beneficiary information:

    (a) the name of the *originator* and the beneficiary;
    (b) the account numbers of the *originator* and the beneficiary, where an account is used to process the *VA transfer*;
    (c) the address of the beneficiary, the number of a government-issued document evidencing the beneficiary's identity, *customer* identification number or date and place of birth; and
    (d) where an account is not used to process the *transfer*, the unique transaction identifier which permits the traceability of the transaction.

40. Further rules and guidance relating to *transfers* with missing or incomplete information is included within Section 18.6.4.

41. Prior to making the *VA*s available to the beneficiary, the *beneficiary VASP* must verify the accuracy of the above information regarding the beneficiary of the *transfer*, using data or documentation.

42. Where a *VA transfer* is made to a self-hosted address, the *beneficiary VASP* must obtain and hold information referred to in Commission Rule 18.39 and ensure that the *VA transfer* can be individually identified.

43. Where a *VA transfer* of £1,000 or more is made to a self-hosted address, the *beneficiary VASP* must take adequate measures to assess if such address is owned or controlled by the beneficiary.

44. Where a *transfer* is carried out which is under the £1,000 threshold, the *beneficiary VASP* must obtain:

    a) the name of the *originator* and the beneficiary; and
    b) the *VA* wallet address for each or a unique transaction reference number,

    but it is not necessary to verify the *customer* information on the *originator* unless the *virtual assets* to be transferred have been received anonymously, or the *VASP* has reasonable grounds for suspecting *ML*, *TF* and/or *PF*.

18.6.4 *Transfers* of *VA*s with missing or incomplete information on the *originator* or the beneficiary

45. In accordance with Paragraph 15D of *Schedule 3*, a *beneficiary VASP* shall –

    (a) before making a *virtual asset* available to a beneficiary –

        (i) monitor the completeness of the *originator* information, and
        (ii) take remedial action where the information specified in (i) is incomplete,

    (b) have risk-based policies for –

        (i) determining when to reject, suspend or otherwise refuse to execute *virtual asset transfers* because of information deficiencies, and
        (ii) the taking of appropriate follow-up action, and

(c) report to *the Commission* repeated failures by an *originating VASP*, *beneficiary VASP* or *intermediary VASP* to comply with the requirements of *Schedule 3* as to the obtaining, holding, verification, retention, provision and use of information in respect of *virtual asset transfers*.

46. The *beneficiary VASP* must have effective procedures and/or systems in place to detect whether the required information is obtained on a *VA transfer* and to detect missing information on both the *originator* and the beneficiary.

47. The *beneficiary VASP*'s policies, procedures and controls should:

(a) take into account the *ML, TF* and *PF risks* to which it is exposed;
(b) set out which *transfers* will be monitored in real time and which can be monitored ex-post and why; and
(c) set out what *employees* should do where the information is missing or incomplete.

48. The level of monitoring should be appropriate to the *risk* of the *VASP* being used in connection with *ML, TF* or *PF*, with high *risk transfers* monitored in real time.

49. Where the *beneficiary VASP* becomes aware that the information is missing or incomplete, the *beneficiary VASP* must, prior to making the *VA*s available to the beneficiary:

(a) ask for and obtain the required information on the *originator* and the beneficiary;
(b) reject the *transfer* prior to the *VA*s being received; or
(c) return the transferred *VA*s to the *originator*'s *VA* account if already received.

50. Where a *VASP* repeatedly fails to provide the required information on the *originator* or the beneficiary, the *beneficiary VASP* must:

(a) take steps to obtain the required information, including, but not limited to,
(i) the issuing of a warning and setting of deadlines;
(ii) reject any future *transfers* from, or to, a *VASP* that fails to provide the required information, and/or
(iii) restrict or terminate its business relationship with a *VASP* that fails to provide the required information; and
(b) notify *the Commission* of that failure and which of the above steps it has taken.

18.6.5 *Intermediary VASP*s

51. In accordance with Paragraph 15C(3) of *Schedule 3*, in respect of any *virtual asset transfer*, an *intermediary VASP* shall –

(a) take reasonable measures which are consistent with straight-through processing to identify *transfers* received by it that are not accompanied by the *originator* and beneficiary information specified in 15C(1)(a),
(b) report to *the Commission* repeated failures by an *originating VASP*, *beneficiary VASP* or *intermediary VASP* to comply with the requirements of *Schedule 3* as to the obtaining, holding, verification, retention, provision and use of information in respect of *virtual asset transfers*,
(c) ensure that any beneficiary information and *originator* information accompanying the *transfer* is retained with it,
(d) subject to (e), ensure the information specified in (c) accompanies the onward *transfer* that the *intermediary VASP* will be making,
(e) where technical limitations prevent the information specified in (c) from accompanying an onward *transfer*, keep a comprehensive record of all information received from the *originating*

VASP or another *intermediary VASP* for a period of not less than five years starting from the date of receipt of the *virtual asset* by the *intermediary VASP*, and

(f) have risk-based policies for:

(i) determining when to reject, suspend or otherwise refuse to execute *virtual assets transfers* because of information deficiencies, and
(ii) the taking of appropriate follow-up action.

52. In respect of any *virtual asset transfer*, an *intermediary VASP* must:

(a) implement effective procedures including, where appropriate, monitoring after or during *transfers*, to detect whether the information on the *originator* or the beneficiary is submitted previously, simultaneously or concurrently with the *VA transfer* or batch file *transfer*, including where the *transfer* is made from or to a self-hosted address; and
(b) take reasonable measures to identify *transfers* which lack required *originator* or beneficiary information.

53. Where the *intermediary VASP* becomes aware that the information is missing or incomplete, the *VASP* must, prior to making the *VA transfer*:

(a) reject the *transfer* and return the transferred *VA*s where in the *intermediary VASP*'s possession; or
(b) ask for and obtain the required information on the *originator* and the beneficiary.

54. Where a *VASP* repeatedly fails to provide the required information on the *originator* or the beneficiary, the *intermediary VASP* must:

(a) take steps to obtain the required information, including, but not limited to,
(i) the issuing of a warning and setting of deadlines;
(ii) reject any future *transfers* from, or to, a *VASP* that fails to provide the required information, and/or
(iii) restrict or terminate its business relationship with a *VASP* that fails to provide the required information; and
(b) notify *the Commission* of that failure and which of the above steps it has taken.

18.6.6 Record retention

55. Both the *originating VASP* and the *beneficiary VASP* must keep records of the complete *originator* and beneficiary information for each *VA transfer* for at least five years.

56. In addition, where technical limitations prevent an *intermediary VASP* from sending the required *originator* or beneficiary information with a *VA transfer*, the *intermediary VASP* must keep records of all information received for at least 5 years.

18.7. Reporting

57. Irrespective of the capacity within which the *VASP* is acting, i.e. *originating VASP*, *beneficiary VASP* or *intermediary VASP*, there are three distinct reporting requirements which are that:

(a) missing or incomplete information on a *transfer* which may give rise to a suspicion of *ML, TF* or *PF* where that suspicion should be reported to the *FIU*;
(b) breaches by a *VASP* of the requirements of paragraphs 15C, 15D or 15E of Schedule 3 and rules in the *Handbook* should be reported to *the Commission*; and

(c) repeated failure by a *VASP* to provide the required *originator* or beneficiary information should be reported to *the Commission*.

18.7.1. Reporting Suspicions and Sanction screening

58. Beneficiary and *intermediary VASP*s should take into account missing or incomplete information on the *originator* or the beneficiary as a factor when assessing whether a *VA transfer*, or any related transaction, is suspicious and whether it is to be reported to the *FIU*. For further information on reporting suspicion, reference should be made to Chapter 13 of this *Handbook* on reporting suspicion.

59. *VASP*s should implement mechanisms to ensure that transactions are scrutinised effectively to identify any suspicious transactions to report to the FIU and screening transactions to meet sanctions obligations to report to the Policy and Resources Committee, as required (see chapter 12 on sanctions). *VASP*s should consider reviewing a combination of the other *customer* information, transaction history and additional transaction data obtained either from the *customer* directly, or from the counterparty *VASP* within the implemented mechanisms.

60. *The Commission* would expect the *VASP*'s internal reporting procedures to apply where an *employee* of a *VASP* forms a suspicion that a *transfer* may be connected to *ML, TF* and/or *PF*, or that funds are derived from the *proceeds* of crime or are terrorist property.

61. *Employees* who are involved in the handling or processing of *transfers* would be considered *relevant employees* for AML/CFT/CPF training purposes and a *VASP* should ensure that its training programme includes training to meet the requirements of Chapter 15 on employee screening and training in this *Handbook*, as well as the *VASP*'s policies, procedures and controls on handling *transfers* of funds and reporting suspicion.

18.7.2. Reporting Breaches

62. A *VASP* must establish policies and procedures for the internal reporting by *employees* of breaches of this *Handbook*, and maintain a record of those breaches and action taken. Such policies and procedures must ensure sufficient confidentiality and protection for *employees* who report breaches committed within the *VASP*.

63. The *board* of a *VASP* should consider notifying *the Commission* in accordance with the requirements of *Commission Rule* 2.63 of any failure by it (the *VASP*) to comply with this *Handbook*.

64. Notifications to *the Commission* should be made promptly and contain the following information:

(a) the specific provision in this *Handbook* and all of the *VASP*'s policies, procedures and controls which have been breached;
(b) the nature of the breach, including its cause;
(c) the date the breach was identified by the *VASP*; and
(d) where possible a summary of the measures taken by the *VASP* in relation to the breach and any subsequent changes to its policies, procedures and controls to mitigate against a recurrence.

65. In order to ensure that the breach is reported promptly, a *VASP* should consider filing an initial report covering items (a) to (c) in Paragraph 18.64 above, together with the steps it is considering taking under (d).

18.8. Risks Associated with the *Virtual Assets* Sector

66. Due to certain characteristics, such as anonymity, immediacy with which a *virtual asset* can be transferred, ease, irrevocability and decentralisation, *VA*s are often associated with illicit activities and *ML* as well as providing an additional means for *TF* and *PF*. Furthermore, the nature of this payment service means that as well as establishing *business relationships* with their *customers*, *VASP*s also carry out *occasional transactions*, where their understanding of the *ML*, *TF* and *PF risk* associated with the *customer* may be limited because there is no ongoing relationship.

67. Decentralised *VASP*s have no central oversight body. AML compliance software is being developed to monitor and identify suspicious transaction patterns, but is not yet commercially tested and available. Conversely, software products have been developed to enhance decentralised *VASP*s' anonymity features, including coin mixers and IP address anonymisers and the use of these tools may make application of *CDD* measures nearly impossible.

68. *Firm*s should be aware of the following *risk* factors alongside those set out in Paragraph 3 of *Schedule 3* and Chapter 3 of this *Handbook*.

18.8.1 Product, Service and Transaction Risk Factors

69. The following factors may contribute to increasing *risk*:

(a) transactions are often fast, simple and irreversible;
(b) the product or service has a global reach, including to high risk jurisdictions or potentially to breach sanctions;
(c) the transaction is cash-based, involves *VA*s or is funded with anonymous electronic money and does not necessarily rely upon other regulated entities;
(d) products are largely unregulated in many jurisdictions;
(e) where *occasional transactions* are undertaken, they take place outside of an established *business relationship* that could otherwise be more readily monitored for uncharacteristic behaviour;
(f) products and techniques that can be used to facilitate anonymity (AECs, mixing and tumbling services, clustering of wallet addresses and privacy wallets), or to exploit a false identity;
(g) transactions that appear to have no obvious economic or financial basis;
(h) unusual, complex or uncharacteristically large transactions;
(i) transactions that route through third countries or third parties, including mixers;
(j) transactions that can be traced to or from the dark web or mixing/tumbler services;
(k) transactions accompanied by information that appears false or contradictory;
(l) *transfers* to the same person from different individuals or to different persons from the same individual with no reasonable explanation;
(m) decentralised *VASP*s are particularly vulnerable to anonymity risks, e.g. by design, certain *VA* wallet addresses that function as accounts, may have no names or *customer* identification attached and the system may have no central server or service provider;
(n) historical transaction chains generated on blockchain are not necessarily associated with the identified *customer*;
(o) transactions can present challenges in tracing the flow of *VA*s and freezing or seizing illicit proceeds held as *VA*s due to data encryption;
(p) *VA*s are deposited soon after registration and withdrawn again shortly after without making use of the services/products of the *VASP*, or are deposited and left dormant;
(q) transactions are conducted that are inconsistent with reasonable trading patterns/strategies, or at specific times and amounts that are not in line with normal industry practices; and/or
(r) the holder of a private key in relation to *VA*s is able to control and *transfer* the *VA*s at any given point in time, the holder of the private key can change and therefore makes the private key similar to a bearer instrument. As such, risks relating to bearer instruments are applicable to *VA*s.

18.8.2 Customer Risk Factors

70. The following factors may contribute to increasing *risk*:

(a) the *customer's* business activity:

(i) the *customer* owns or operates a business that handles large amounts of cash or *VA*s; and/or
(ii) the *customer's* business has a complicated ownership structure.

(b) the *customer's* behaviour:

(i) the *customer's* needs may be better serviced elsewhere, for example, because the *VASP* is not local to the *customer* or the *customer's* business;
(ii) the *customer* offers false, fraudulent or fictitious identification information or documents;
(iii) the *customer* delays producing identification documents or other requested information without suitable justification, or cancels a transaction after learning of a *CDD* requirement;
(iv) the *customer's* behaviour makes no apparent economic sense, for example, the *customer* accepts a poor exchange rate or high charges unquestioningly, requests a transaction in a currency that is not official tender or commonly used in the jurisdiction where the *customer* and/or recipient is located or requests or provides large amounts of currency in either low or high denominations;
(v) the *customer's* transactions are always just below applicable thresholds, including the £1,000 threshold for *occasional transactions* set out in *the Law*;
(vi) the *customer's* use of the service is unusual, for example, they send or receive *VA*s to or from themselves or send *VA*s on immediately after receiving them;
(vii) the *customer* appears to know little or is reluctant to provide information about the beneficiary;
(viii) several of the firm's *customers transfer funds* to the same beneficiary or appear to have the same identification information, for example, address or telephone number;
(ix) an incoming transaction is not accompanied by the required information on the *originator* or beneficiary;
(x) the amount sent or received is at odds with the *customer's* income (if known);
(xi) the *customer* makes use of mixing/tumbler services or similar, or engages in transactions that can be traced to the dark web;
(xii) the *customer* is a legal person which cannot be found on the internet and/or uses an email address with an unusual domain part such as Hotmail, Gmail, Yahoo etc. especially if the *customer* is otherwise secretive or avoids direct contact;
(xiii) the *customer* uses proxies or unverifiable IP addresses or uses disposable email addresses or mobile numbers;
(xiv) the *customer* uses different devices to conduct transactions to obscure their actual location or circumvent restrictions;
(xv) the *customer* uses multiple wallets for the same *virtual assets* or changes wallets for the same *virtual asset*;
(xvi) the *customer* is a business or NPO which transacts with the *VASP* in a manner expected of individuals, which could indicate a front or shell company or be indicative of misappropriation of funds;
(xvii) the *customer*'s IP address either appears to be connected to a VPN or other similar IP anonymisers, changes repeatedly, or does not agree to other information held by the firm on the c*ustomer*'s location;
(xviii) the *customer* is part of a complex structure that makes the determination of the beneficial owner more difficult; and/or
(xix) the bank account or payment card linked to the *customer*'s account is changed often.

18.8.3 Country or Geographical Risk Factors

71. The following factors may contribute to increasing *risk*:

    (a) The *originator* or the beneficiary is located in a jurisdiction associated with higher *ML*, *TF* and/or P*F risk*;
    (b) The beneficiary is resident in a jurisdiction that has no, or a less developed, formal banking sector, which means that informal money remittance services, such as hawala, may be used at point of payment;
    (c) *VASP*s based in other jurisdictions may not require a user to be identified and their identity verified; and/or
    (d) *VASP*s based in other jurisdictions may not be regulated, or may have regulatory requirements that do not meet, or insufficiently meet, FATF Standards.

18.8.4 Distribution Channel Risk Factors

72. The following factors may contribute to increasing *risk*:

    (a) there are no restrictions on the funding instrument, for example, cash, unrestricted E-money products, *wire transfers*, cheques or *VA*s;
    (b) there is a lack of face-to-face contact with the *customer* and any persons associated with them;
    (c) the distribution channel used provides a degree of anonymity;
    (d) the service is provided entirely online without adequate safeguards;
    (e) the *VA* service is provided through agents that:

        (i) represent more than one principal;
        (ii) have unusual turnover patterns compared with other agents in similar locations, for example, unusually high or low transaction sizes, unusually large cash transactions or a high number of transactions that fall just under the *CDD* threshold, or undertake business outside normal business hours;
        (iii) undertake a large proportion of business with *originator*s or beneficiaries from jurisdictions associated with higher *ML*, *TF* and/or P*F risk*;
        (iv) appear to be unsure about, or inconsistent in, the application of group-wide AML, CFT and CPF policies; or
        (v) are not from the financial sector and conduct another business as their main business;

    (f) the *VA* service is provided through a large network of agents in different jurisdictions; and/or
    (g) the *VA* service is provided through an overly complex payment chain, for example, with a large number of intermediaries operating in different jurisdictions or allowing for untraceable (formal and informal) settlement systems;

Appendix A

Glossary of Terms

The below list of terms includes those defined within *Schedule 3*, together with additional definitions of other terms used within this *Handbook*. Unless the context otherwise requires, terms within this *Handbook* should be read as having the following definition.

Any reference to an enactment is to that enactment as from time to time amended, repealed and replaced, extended or applied by or under any other enactment.

"the 2020 Regulations" means the Sanctions (Implementation of UK Regimes) (Bailiwick of Guernsey) (Brexit) Regulations, 2020.

"**account**" means a *bank* account and any other *business relationship* between a *specified business* and a *customer* which is of a similar nature having regard to the services offered by the *specified business*.

"**the Amendment Ordinance**" means the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) Ordinance, 2018.

"**Appendix C business**" means:

(a) a *financial services business* supervised by *the Commission*, or

(b) a business which is carried on from:

(i) a country or territory listed in Appendix C to this *Handbook* and which would, if it were carried on in *the Bailiwick*, be a *financial services business*, or

(ii) the United Kingdom, the Bailiwick of Jersey, *the Bailiwick* or the Isle of Man by a lawyer or an accountant,

and, in either case, is a business:

(A) which may only be carried on in that country or territory by a person regulated for that purpose under the law of that country or territory,

(B) the conduct of which is subject to requirements to forestall, prevent and detect *ML*, *TF* and *PF* that are consistent with those in *the FATF Recommendations* in respect of such a business, and

(C) the conduct of which is supervised for compliance with the requirements referred to in (B), by *the Commission* or an overseas regulatory authority.

"**the Bailiwick**" means the Bailiwick of Guernsey.

"**bank**" means a person who accepts deposits, including a person who does so in a country or territory outside *the Bailiwick*, in the course of carrying on a deposit-taking business within the meaning of *the Banking Law* and related expressions shall be construed accordingly.

"**the Banking Law**" means the Banking Supervision (Bailiwick of Guernsey) Law, 2020.

"**batch transfer**" means a transfer comprised of a number of individual virtual asset transfers from one or more *originators* that are being sent to the same *VASP*, but may or may not be ultimately intended for different persons.

"**bearer share**" means a negotiable instrument that accords ownership in a *legal person* to the individual who possesses the relevant bearer share certificate.

"**bearer warrant**" means a warrant or other instrument entitling the holder to subscribe for shares or other investments in the capital of a company, title of which can be transferred by delivery.

"**beneficial owner**" has the meaning in Paragraph 22 of *Schedule 3*.

"**the Beneficial Ownership Law**" means the Beneficial Ownership of Legal Persons (Guernsey) Law, 2017.

"**the Beneficial Ownership Regulations**" means the Beneficial Ownership (Definition) Regulations, 2017.

"**beneficiary VASP**" means the *VASP* which receives the transfer of *virtual assets* from the *originating VASP* directly or through an *intermediary VASP* and makes the virtual asset available to the beneficiary.

"**board**", in relation to a *specified business*, means:

(a) the board of directors of that *specified business*, where it is a body corporate, or
(b) the senior management of that *specified business*, where it is not a body corporate,

and references to the board of a *specified business* shall, where the *specified business* is a sole trader, be construed consistently with the provisions of this *Handbook*.

"**branch office**" of a business means a place of business of that business that is physically separate from that business and that has no legal personality.

"**British Islands**" means *the Bailiwick*, the UK, the Bailiwick of Jersey and the Isle of Man.

"**business relationship**" means a business, professional or commercial relationship between a *specified business* and a *customer* which is expected by the *specified business*, at the time when contact is established, to have an element of duration. Such a relationship does not need to involve the firm in an actual transaction; giving advice may often constitute establishing a business relationship.

"**business risk assessment**" means, in accordance with Paragraph 3(3) of *Schedule 3*, an assessment which is appropriate to the nature, size and complexity of the firm and which is in respect of:

(a) *customers*, and the *beneficial owners* of *customers*,
(b) countries and geographic areas, and
(c) products, services, transactions and delivery channels (as appropriate), and in particular in respect of the *ML, TF* or *PF* risks that may arise in relation to -

    (i) the development of new products and new business practices, before such products are made available and such practices adopted, and
    (ii) the use of new or developing technologies for both new and pre-existing products, before such technologies are used and adopted,

and the *business risk assessments* must include (without limitation) consideration of the implications for, and risks to, the business of the offences specified in the *NRA* as being the most likely predicate offences of the Bailiwick being used for *money laundering*, *terrorist financing* or *proliferation financing*.

"**the Commission**" means the Guernsey Financial Services Commission established by *the Financial Services Commission Law*.

"**Commission Rules**" has the meaning in Paragraph 1.17.(a) of this *Handbook*.

"**the Code**" means the *Commission's* Finance Sector Code of Corporate Governance.

"**consolidated supervision**" means supervision by a regulatory authority of all aspects of the business of a group of bodies corporate carried on worldwide, to ensure compliance with:

(a) *the FATF Recommendations*; and
(b) other international requirements,

and in accordance with the Core Principles of Effective Banking Supervision issued by the Basel Committee on Banking Supervision as revised or reissued from time to time.

"**correspondent banking relationship**" means a *business relationship* which involves the provision of banking services by one *bank* to another *bank* ("the respondent *bank*").

"**Crown Dependencies**" means the *Bailiwick*, the Bailiwick of Jersey and the Isle of Man.

"**customer**" means a person or *legal arrangement* who:

(a) is seeking to establish, or has established, a *business relationship* with a *specified business*, or
(b) is seeking to carry out, or has carried out, an *occasional transaction* with a *specified business*,

except that where such a person or *legal arrangement* is an *introducer*, the *customer* is the person or *legal arrangement* on whose behalf the *introducer* is seeking to establish or has established the *business relationship*.

"**customer due diligence**" or "**CDD**" means the steps which a *specified business* is required to carry out pursuant to Paragraph 4(3) of *Schedule 3*, being that:

(a) the *customer* shall be identified and the identity of the *customer* verified using *identification data*,
(b) any person purporting to act on behalf of the *customer* shall be identified and that person's identity and authority to so act shall be verified,
(c) the *beneficial owner* shall be identified and reasonable measures shall be taken to verify such identity using *identification d*ata and such measures shall include, in the case of a *customer* which is a *legal person* or *legal arrangement*, measures to understand the nature of the customer's business and its ownership and control structure,
(d) a determination shall be made as to whether the *customer* is acting on behalf of another person and, if the *customer* is so acting, reasonable measures shall be taken to identify that other person and to obtain sufficient *identification data* to verify the identity of that other person,
(e) the purpose and intended nature of each *business relationship* and *occasional transaction* shall be understood, and information shall be obtained as appropriate to support this understanding, and
(f) a determination shall be made as to whether the *customer* or *beneficial owner* is a *PEP*, and, if so, whether he or she is a *foreign PEP*, a *domestic PEP* or a person who is or has been entrusted with a prominent function by an *international organisation*.

"**customer due diligence information**" or "**CDD information**" means:

(a) *identification data*;

(b) any *account* files and correspondence relating to the *business relationship* or *occasional transaction*; and
(c) all records obtained through *CDD* measures, including the results of any analysis undertaken.

"**the Data Protection Law**" means the Data Protection (Bailiwick of Guernsey) Law, 2017.

"**the Disclosure Law**" means the Disclosure (Bailiwick of Guernsey) Law, 2007.

"**the Disclosure Regulations**" means the Disclosure (Bailiwick of Guernsey) Regulations, 2007.

"**document**" includes data or information recorded in any form (including, without limitation, in electronic form).

"**domestic PEP**" has the meaning set out in the definition of *Politically Exposed Person*.

"**the Drug Trafficking Law**" means the Drug Trafficking (Bailiwick of Guernsey) Law, 2000.

"**EFCB**" means the Economic and Financial Crime Bureau established by the States of Guernsey Committee for Home Affairs in June 2021.

"**employee**" means an individual working, including on a temporary basis, for a *specified business* whether under a contract of employment, a contract for services or otherwise. For the purposes of this *Handbook*, references to *employee* include any partner of the *specified business*.

"**the Enforcement Law**" means the Financial Services Business (Enforcement Powers) (Bailiwick of Guernsey) Law, 2020.

"**enhanced customer due diligence**" or "**ECDD**" means, in accordance with Paragraph 5(3)(a) of *Schedule 3*:

(i) obtaining senior management approval for establishing a *business relationship* or undertaking an *occasional transaction*,
(ii) obtaining senior management approval for, in the case of either -
    (A) an existing *business relationship* with a foreign *PEP*, or
    (B) an existing high *risk business relationship* with a *domestic or international organisation PEP*,
continuing that relationship,
(iii) taking reasonable measures to establish and understand the source of any *funds* and of the wealth of –

    (A) the *customer*, and
    (B) the *beneficial owner*, where the *beneficial owner* is a *PEP*,

(iv) carrying out more frequent and more extensive ongoing monitoring, including increasing the number and timing of controls applied and selecting patterns of activity or transactions that need further examination, in accordance with Paragraph 11 of *Schedule 3*, and
(v) taking one or more of the following steps as would be appropriate to the particular *business relationship* or *occasional transaction* -

    (A) obtaining additional information about the *customer*, such as the type, volume and value of the *customer's* assets and additional information about the *customer's beneficial owners*,
    (B) verifying additional aspects of the *customer's* identity,

(C) obtaining additional information to understand the purpose and intended nature of each *business relationship* and *occasional transaction*, and
(D) taking reasonable measures to establish and understand the source of funds and wealth of *beneficial owners* not falling within (c) above.

"**enhanced measures**" means, in accordance with Paragraph 5(3)(b) of *Schedule 3*, the carrying out of appropriate and adequate enhanced measures in relation to a *business relationship* or *occasional transaction*, to mitigate and manage the specific higher *risk* of *ML*, *TF* and *PF* resulting from the matters listed in Paragraph 5(2) of *Schedule 3* that are relevant to that relationship or transaction.

"**the EU Regulation**" means Regulation (EU) 2015/847 on Information Accompanying Transfers of Funds.

"**express trust**" means a trust clearly created by the settlor, usually in the form of a *document*, for example, a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangement (for example, a constructive trust).

"**the FATF Recommendations**" means the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation issued by the Financial Action Task Force as revised or reissued from time to time.

"**the Fiduciaries Law**" means the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc. (Bailiwick of Guernsey) Law, 2020.

"**financial exclusion**" means individuals being prevented from having access to essential financial services, such as banking services, because they are unable, for valid reasons, to produce more usual *CDD* documentation.

"**Financial Intelligence Unit**" or "**FIU**" means the competent authority for the receipt, analysis and dissemination within *the Bailiwick*, and elsewhere, of disclosures under Part I of *the Disclosure Law* and Part III of *the Terrorism Law* which are more commonly known or referred to as suspicious transaction reports or suspicious activity reports.

"**financial services business**" or "**FSB**" means any business specified in Schedule 1 to *the Law* and includes, unless the context otherwise requires, a person carrying on such a business in *the Bailiwick* or an *Appendix C business* conducting business equivalent to that specified in Schedule 1 to *the Law*. For the avoidance of doubt, a business is a financial services business only in respect of the businesses specified in Schedule 1, and only to the extent that it conducts one or more of those businesses.

"**the Financial Services Commission Law**" means the Financial Services Commission (Bailiwick of Guernsey) Law, 1987.

"**fixed trust**" means a trust in respect of which the beneficiaries of the trust, and the interests of those beneficiaries, are certain.

"**foreign PEP**" has the meaning set out in the definition of *Politically Exposed Person*.

"**forming a suspicion**" of *ML*, *TF* or *PF*, and any related expressions, are references to a person –

(a) knowing or suspecting, or
(b) having reasonable grounds for knowing or suspecting,

that another person is engaged in –

(i) *ML* or that certain property is or is derived from the proceeds of criminal conduct (within the meaning of *the Disclosure Law*),
(ii) *FT* or that certain property is or is derived from terrorist property (within the meaning of *the Terrorism Law*), or
(iii) *PF* (within the meaning of Section 16A of *the Law*).

as the case may be.

"**foundation**" means -

(a) a foundation created under the Foundations (Guernsey) Law, 2012, or
(b) an equivalent or similar body created or established under the law of another jurisdiction (and howsoever named).

"**foundation official**" means -

(a) in relation to a foundation created under the Foundations (Guernsey) Law, 2012, a foundation official within the meaning of that Law, and
(b) in relation to an equivalent or similar body created or established under the law of another jurisdiction, a person with functions corresponding to those of a foundation official described in paragraph (a).

"**founder**" means -

(a) in relation to a foundation created under the Foundations (Guernsey) Law, 2012, a founder within the meaning of that Law; and
(b) in relation to an equivalent or similar body created or established under the law of another jurisdiction, a person corresponding to a founder described in paragraph (a).

"**the FSB Regulations**" means the Criminal Justice (Proceeds of Crime) (Financial Services Business) (Bailiwick of Guernsey) Regulations, 2007, which have been repealed.

"**funds**" means assets of all types, and documents or instruments evidencing title to or interest in such assets.

"**guidance**" has the meaning in Paragraph 1.19.(b) of this *Handbook*.

"**Handbook**" means this Handbook, as revised or re-issued from time to time by *the Commission*.

"**high risk relationship**" means a *business relationship* or an *occasional transaction* which has a high *risk* of involving *ML, TF* or *PF* and related terms shall be construed accordingly.

"**the IB Law**" means the Insurance Business (Bailiwick of Guernsey) Law, 2002.

"**identification data**" means *documents*, data and information from a reliable and independent source.

"**the IMII Law**" means the Insurance Managers and Insurance Intermediaries (Bailiwick of Guernsey) Law, 2002.

"**intermediary**" means an *FSB* which is considered to be the *customer* of a *specified business* when establishing a *business relationship* or undertaking an *occasional transaction* in accordance with the provisions of Section 9.8. of this *Handbook*.

"**the Information Regulations**" means collectively the Disclosure (Bailiwick of Guernsey) (Information) Regulations, 2019 as amended and the Terrorism and Crime (Bailiwick of Guernsey) (Information) Regulations, 2019 as amended.

"**intermediary relationship**" means a *business relationship* in which the *customer* is an *intermediary*.

"**intermediary VASP**" means a *VASP* which is not acting on behalf of the *originator* or beneficiary but receives or transmits a *virtual asset* on behalf of the *originating VASP*, the *beneficiary VASP*, or another intermediary *VASP*.

"**international organisation**" means an entity –

(a) which was established by a formal political agreement between its member states that has the status of an international treaty,
(b) the existence of which is recognised by law in its member states, and
(c) which is not treated as a resident institutional unit of the country in which it is located.

"**international organisation PEP**" or "**IOPEP**" has the meaning set out in the definition of *Politically Exposed Person*.

"**introducer**" means an *Appendix C business* who is seeking to establish or has established, on behalf of another person or *legal arrangement* who is its *customer*, a *business relationship* or undertake an *occasional transaction* with a *specified business.*

"**joint arrangement**" means, in accordance with Regulation 5 of *the Beneficial Ownership Regulations*:

(1) if shares or rights in a *relevant legal person* or other legal entity held by a person and shares or rights in the same person or other entity held by another person are the subject of a joint arrangement between those persons, each of them is treated as holding the combined shares or rights of both of them.
(2) a "joint arrangement" is an arrangement between the holders of shares (or rights) in a *relevant legal person* or other legal entity that they will exercise all or substantially all the rights conferred by their respective shares (or rights) jointly in a way that is pre-determined by the arrangement.
(3) "arrangement" includes-

    (a) any scheme, agreement or understanding, whether or not it is legally enforceable, and
    (b) any convention, custom or practice of any kind.

(4) but something does not count as an arrangement unless there is at least some degree of stability about it (whether by its nature or terms, the time it has been in existence or otherwise).

"**joint interests**" means, in accordance with Regulation 4 of *the Beneficial Ownership Regulations*, that if two or more persons each hold a share or right in a *legal person* or other legal entity jointly, each of them is treated as holding that share or right.

"**key principal**" means, in the context of a *business relationship* or *occasional transaction*, a natural person, *legal person* or *legal arrangement* falling within one or more of Paragraphs 4(3)(a)-(d) of *Schedule 3* in respect of that *business relationship* or *occasional transaction*, specifically:

(a) the *customer*;

(b) any person purporting to act on behalf of the *customer*;
(c) the *beneficial owner* of the *customer*; and
(d) any person on behalf of whom the *customer* is acting.

"**the Law**" means the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999.

"**the LCF Law**" means the Lending, Credit and Finance (Bailiwick of Guernsey) Law, 2022.

"**legal arrangement**" includes an *express trust* and any vehicle or arrangement whatsoever which has a similar legal effect to an *express trust*.

"**legal person**" means bodies corporate, *foundations*, anstalt, partnerships, or associations, or any similar bodies that can establish a *business relationship* or undertake an *occasional transaction* with a *specified business* or otherwise own property.

"**low risk relationship**" means a *business relationship* or an *occasional transaction* which has a low *risk* of involving *ML, TF* or *PF* and related terms shall be construed accordingly.

"**maintain**" means, in the context of the requirements of this *Handbook*, that relevant policies, procedures and controls must be established and implemented, and that the *specified business* must monitor such policies, procedures and controls to ensure that they are operating effectively.

"**minimum retention period**" means:

(a) in the case of any *CDD information*-

  (i) a period of five years starting from the date-

    (A) where the *customer* has established a *business relationship* with the *specified business*, that relationship ceased,
    (B) where the *customer* has carried out an *occasional transaction* with the *specified business*, that transaction was completed, or

  (ii) such other longer period as *the Commission* may direct,

(b) in the case of a *transaction document*-

  (i) a period of five years starting from the date that both the transaction and any related transaction were completed, or
  (ii) such other longer period as *the Commission* may direct.

"**money laundering**" or "**ML**" has the same meaning as "money laundering offence" has in *the Law*, specifically:

(a) an offence under Section 38, 39 or 40 of *the Law*,
(b) an attempt, conspiracy or incitement to commit an offence specified in (a),
(c) aiding, abetting, counselling or procuring the commission of an offence specified in (a), or
(d) an offence committed outside *the Bailiwick* which would constitute an offence specified in (a), (b) or (c) if committed within *the Bailiwick*.

"**Money Laundering Compliance Officer**" or "**MLCO**" means a person of at least manager level appointed by a *specified business* to monitor compliance with policies, procedures and controls to forestall, prevent and detect *ML, TF* and *PF*.

"**Money Laundering Reporting Officer**" or "**MLRO**" means a person of at least manager level appointed by a *specified business* to make or receive disclosures under Part I of *the Disclosure Law* and Sections 12, 15 and 15A of *the Terrorism Law*.

"**National Risk Assessment**" or "**NRA**" means the National Risk Assessment published by the States of Guernsey Policy & Resources Committee as amended from time to time.

"**nominated firm**" means a *specified business* licensed under *the POI Law* nominated by a CIS in accordance with Paragraph 4.59. of this *Handbook*.

"**Nominated Officer**" means a natural person nominated by a *specified business* in accordance with Paragraph 12(1)(b) or 12(1)(c) of *Schedule 3* to receive disclosures under Part I of *the Disclosure Law* and Section 15 of *the Terrorism Law* in the absence of the *MLRO* and otherwise carry out the functions of the *MLRO* in that officer's absence.

"**nominee director**" means, in accordance with Section 7.3.2. of this *Handbook*, a natural or *legal person* holding the position of director on the board of a *legal person* and acting on behalf of another natural or *legal person*.

"**nominee shareholder**" has the same meaning as "nominee" has in the Beneficial Ownership of Legal Persons (Nominee Relationships) Regulations, 2017, specifically a legal or natural person in a nominee relationship in which that person is registered as the legal owner of a share or right in a company (or of an equivalent interest in a *foundation*, limited partnership or LLP) which is held or is exercisable by that person on behalf of a *beneficial owner* of that company, *foundation*, limited partnership or LLP as the case may be, whether directly or indirectly (other than as the trustee of a trust).

"**non-Guernsey collective investment scheme**" or "**NGCIS**" means any open or closed-ended collective investment scheme established outside *the Bailiwick*.

"**notify**" means in writing, and includes for the purposes of this *Handbook*, notifications made to *the Commission* via the PQ Portal and Online Submissions Portal and to the *FIU* via THEMIS.

"**occasional transaction**" means any transaction involving more than £10,000 (or £1,000 or more in the case of a specified business described in paragraph 27(2) of Schedule 1 ("VASPs")), carried out by the *specified business* in question in the course of that business, where no *business relationship* has been proposed or established and includes such transactions carried out in a single operation or two or more operations that appear to be linked.

"**originating VASP**" means the *VASP* which initiates the transfer of the *virtual asset* and transfers the *virtual asset* upon receiving the order for a transfer of the *virtual asset* from or on behalf of the *originator*.

"**originator**" means the customer who allows the transfer of the *virtual asset* from the customer's account or, where there is no account, the person who places the order with the *originating VASP* to perform the transfer.

"**payer**" means a natural person., *legal person* or *legal arrangement* that holds a payment *account* and allows a transfer of *funds* from that payment *account*, or, where there is no payment *account*, that gives a transfer of *funds* order.

"**payee**" means a natural person, *legal person* or *legal arrangement* identified by the *payer* as the intended recipient of the transfer of *funds*.

"**payment service provider**" or "**PSP**" means any business undertaking the activities specified within Paragraphs 4 or 5 of Part I of Schedule 1 to *the Law*.

"**the PB Law**" means the Prescribed Business (Bailiwick of Guernsey) Law, 2008.

"**the PB Regulations**" means the Criminal Justice (Proceeds of Crime) (Legal Professionals, Accountants and Estate Agents) (Bailiwick of Guernsey) Regulations, 2008, which have been repealed.

"**physical presence**" means the presence of persons involved in a meaningful way in the running and management of the *bank* which, for the avoidance of doubt, is not satisfied by the presence of a local agent or junior staff.

"**the POI Law**" means the Protection of Investors (Bailiwick of Guernsey) Law, 2020.

"**police officer**" means, in accordance with Section 51(1) of *the Law* -

(a) in relation to Guernsey, Herm and Jethou, a member of the salaried police force of the Island of Guernsey and, within the limits of his jurisdiction, a member of the special constabulary of the Island of Guernsey,
(b) in relation to Alderney, a member of the said salaried police force, a member of any police force which may be established by the States of Alderney and, within the limits of his jurisdiction, a special constable appointed or deemed to be appointed pursuant to the provisions of an Ordinance made under Section 46A of the Government of Alderney Law, 1987,
(c) in relation to Sark, the Constable, the Vingtenier and a member of the said police force of the Island of Guernsey, and
(d) an officer within the meaning of Section 1(1) of the Customs and Excise (General Provisions) (Bailiwick of Guernsey) Law, 1972.

"**politically exposed person**" or "**PEP**" means, in accordance with Paragraph 5(4) of *Schedule 3*, subject to Paragraphs 5(5) and 5(5A) of *Schedule 3* -

(a) a natural person who has, or has had at any time, a prominent public function, or who has been elected or appointed to such a function, including, without limitation:

    (i) heads of state or heads of government,
    (ii) senior politicians and other important officials of political parties,
    (iii) senior government officials,
    (iv) senior members of the judiciary,
    (v) senior military officers, and
    (vi) senior executives of state owned body corporates,

    (and such a person shall be referred to as a "**foreign PEP**" unless he or she holds or has held or has been elected or appointed to the prominent public function in question in respect of *the Bailiwick*, in which case he or she shall be referred to as a "**domestic PEP**"),
(b) a person who is, or who has been at any time, entrusted with a prominent function by an *international organisation* ("**international organisation PEP**"),
(c) an immediate family member of a person referred to in (a) or (b) including, without limitation, a spouse, partner, parent, child, sibling, parent-in-law or grandchild of such a person and for the purposes of this definition "partner" means a person who is considered by the law of the country or territory in which the relevant public function is held as being equivalent to a spouse, or
(d) a close associate of a person referred to in (a) or (b), including, without limitation:

    (i) a person who is widely known to maintain a close business relationship with such a person, or

(ii) a person who is in a position to conduct substantial financial transactions on behalf of such a person.

"**prescribed business**" or "**PB**" means any business which is a relevant business for the purposes of *the Law*, but does not include a business of a type described in Paragraphs 2 or 4 of Schedule 2 to *the Law*.

"**proceeds**" means any property derived from or obtained, directly or indirectly, through the commission of an offence.

"**proliferation financing**" or "**PF**" means, in accordance with *the Law*, doing any act which breaches targeted financial sanctions that –

(a) are imposed under any international sanctions measure that has been implemented in the Bailiwick and
(b) relate to the proliferation of weapons of mass destruction and its financing,

and for the avoidance of doubt, the breach of targeted financial sanctions includes their non-implementation, circumvention or evasion.

"**protector**" means, in accordance with Section 58 of *the Fiduciaries Law*, in relation to a trust, a person other than a trustee who, as the holder of an office created by the terms of the trust, is authorised or required to participate in the administration of the trust.

"**the Regulatory Laws**" means –

(a) the Banking Supervision (Bailiwick of Guernsey) Law, 2020;
(b) the Insurance Business (Bailiwick of Guernsey) Law, 2002;
(c) the Insurance Managers and Insurance Intermediaries (Bailiwick of Guernsey) Law, 2002;
(d) the Protection of Investors (Bailiwick of Guernsey) Law, 2020;
(e) the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc. (Bailiwick of Guernsey) Law, 2020; and
(f) the Lending, Credit and Finance (Bailiwick of Guernsey) Law, 2022.

"**relationship risk assessment**" means the assessment of *risk* within a *business relationship* or *occasional transaction*.

"**relevant connection**" means, in accordance with Paragraph 5(10) of *Schedule 3*, for the purposes of a *customer* or *beneficial owner* having a relevant connection with a country or territory, the *customer* or *beneficial owner*:

(a) is the government, or a public authority, of the country or territory,
(b) is a *PEP* within the meaning of Paragraph 5(4) of *Schedule 3* in respect of the country or territory,
(c) is resident in the country or territory,
(d) has a business address in the country or territory,
(e) derives *funds* from –

(i) assets held by the *customer* or *beneficial owner*, or on behalf of the *customer* or *beneficial owner*, in the country or territory, or
(ii) income arising in the country or territory, or

(f) has any other connection with the country or territory which the *specified business* considers, in light of that business' duties under *Schedule 3* (including but not limited to its duties under Paragraph 2 of *Schedule 3*), to be a relevant connection for those purposes.

"**relevant employee**" means any –

(a) member of the *board* of the *specified business*,
(b) member of the management of the *specified business*, and
(c) employee whose duties relate to the *specified business*.

"**the Relevant Enactments**" means –

(a) the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999;
(b) the Drug Trafficking (Bailiwick of Guernsey) Law, 2000;
(c) the Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011;
(d) the Sanctions (Bailiwick of Guernsey) Law, 2018;
(j) the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002;
(k) the Disclosure (Bailiwick of Guernsey) Law, 2007;
(l) the Transfer of Funds (Guernsey) Ordinance, 2017;
(m) the Transfer of Funds (Alderney) Ordinance, 2017;
(n) the Transfer of Funds (Sark) Ordinance, 2017;
(o) the Disclosure (Bailiwick of Guernsey) Regulations, 2007;
(p) the Terrorism and Crime (Bailiwick of Guernsey) Regulations, 2007;
(q) the Prescribed Businesses (Bailiwick of Guernsey) Law, 2008;
(r) the Beneficial Ownership of Legal Persons (Guernsey) Law, 2017;
(s) the Beneficial Ownership of Legal Persons (Alderney) Law, 2017;
(t) the Beneficial Ownership (Definition) Regulations, 2017;
(u) the Beneficial Ownership (Alderney) (Definitions) Regulations, 2017;
(v) the Beneficial Ownership of Legal Persons (Provision of Information) (Transitional Provisions) Regulations, 2017;
(w) the Beneficial Ownership of Legal Persons (Provision of Information) (Transitional Provisions) (Alderney) Regulations, 2017;
(x) the Beneficial Ownership of Legal Persons (Nominee Relationships) Regulations, 2017;
(y) the Beneficial Ownership of Legal Persons (Nominee Relationships) (Alderney) Ordinance, 2017;
(z) the Beneficial Ownership of Legal Persons (Provision of Information) (Limited Partnerships) Regulations, 2017;

and such other enactments relating to *ML, TF* and *PF* as may be enacted from time to time in *the Bailiwick.*

"**relevant person**" means, in the context of a *foundation,* the registered agent, *foundation official* or any other person who holds information on the identity of the *beneficial owners* of the *foundation.*

"**relevant legal person**" means, in accordance with Paragraph 41(1) of *the Beneficial Ownership Law*:

(a) a company incorporated under the Companies (Guernsey) Law, 2008,
(b) an LLP incorporated under the Limited Liability Partnerships (Guernsey) Law, 2013,
(c) a *foundation* established under the Foundations (Guernsey) Law, 2012, or
(d) a limited partnership with legal personality registered under the Limited Partnerships (Guernsey) Law, 1995.

"**the Reporting Laws**" means collectively *the Disclosure Law* and *the Terrorism Law.*

"**the Reporting Regulations**" means collectively the Disclosure (Bailiwick of Guernsey) Regulations, 2007 and the Terrorism and Crime (Bailiwick of Guernsey) Regulations, 2007.

"**risk**" means a risk of *ML, TF* or *PF* occurring and "**risk assessment**" shall be construed accordingly.

"**risk appetite**" means, in accordance with Paragraph 3(2)(b) of *Schedule 3*, the type and extent of the *risks* that a *specified business* is willing to accept in order to achieve its strategic objectives.

"**satisfied**" means, in the context of a *specified business* being satisfied as to a matter, that the *specified business* must be able to justify and demonstrate its assessment to *the Commission*.

"**Schedule 3**" means Schedule 3 to *the Law*.

"**settlor**" means any natural person, *legal person* or *legal arrangement* who transfers ownership of their assets to a trustee.

"**shell bank**" means a *bank* that has no *physical presence* in the country or territory in which it is incorporated and licensed and which is not a member of a group of bodies corporate which is subject to effective *consolidated supervision*.

"**simplified customer due diligence**" or "**SCDD**" has the meaning in Paragraph 6 of *Schedule 3*.

"**specified business**" means, in accordance with Paragraph 1(1) of *Schedule 3* and for the purposes of *Schedule 3* and this *Handbook*, a *financial services business* or a *prescribed business*.

"**subordinate legislation**" means any ordinance, statutory instrument, paragraph, rule, order, notice, rule of court, resolution, scheme, warrant, byelaw or other instrument made under any enactment and having legislative effect.

"**termination**" means the conclusion of a relationship between a *specified business* and the *customer*. In the case of a *business relationship*, termination occurs on the closing or redemption of a product or service or the completion of the last transaction. With an *occasional transaction*, termination occurs on completion of that *occasional transaction* or the last in a series of linked transactions or the maturity, claim on or cancellation of a contract or the commencement of insolvency proceedings against a *customer*.

"**the Terrorism Law**" means the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002.

"**the Terrorist Asset-Freezing Law**" means the Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011.

"**terrorist financing**" or "**TF**" means, in accordance with *the Terrorism Law*, doing any act which –

(a) constitutes an offence under Section 8, 9, 10, 11 or 11A of *the Terrorism Law*, or Section 9, 10, 11, 12 or 13 of *the Terrorist Asset-Freezing Law*, or an offence under Section 3 of the Sanctions (Bailiwick of Guernsey) Law, 2018 in respect of the relevant UK sanctions regimes implemented by the Sanctions (Implementation of UK Regimes) (Bailiwick of Guernsey) (Brexit) Regulations, 2020 and, for the purposes of this definition, the "purposes of terrorism" shall include, to the extent that they do not already do so –

  (i) any attempt, conspiracy or incitement to carry out terrorism within the meaning of Section 1 of *the Terrorism Law*, or
  (ii) aiding, abetting, counselling or procuring the carrying out of such terrorism,

(b) constitutes an attempt, conspiracy or incitement to commit an offence specified in (a),
(c) constitutes aiding, abetting, counselling or procuring the commission of an offence specified in (a), or
(d) would, in the case of an act done otherwise than in *the Bailiwick*, constitute an offence specified in (a), (b) or (c) if done in *the Bailiwick*,

irrespective of the value of the property involved, and for the purposes of this definition having possession of any property shall be taken to be doing an act in relation to it.

"**transaction document**" means, in accordance with Paragraph 14 of *Schedule 3*, a comprehensive record of a transaction with a *customer* or an *introducer*, including the amounts and types of currency involved in the transaction (if any).

"**transfer**" in respect of a *virtual asset* means a transaction carried out on behalf of an *originator* through an *originating VASP* by electronic means with a view to making a *virtual asset* available to a beneficiary at a *beneficiary VASP*, irrespective of whether the *originator* and the beneficiary are the same person.

"**transfer agent**" means the financial institution assigned by a CIS to maintain records of investors into that CIS, together with their associated *account* balances.

"**the Transfer of Funds Ordinance**" means the Transfer of Funds (Guernsey, Sark or Alderney) Ordinance, 2017 relevant to the island within which the *specified business* is operating.

"**transparent legal person**" means, in accordance with Paragraph 22(10) of *Schedule 3*:

(a) a company that is listed on a recognised stock exchange within the meaning of *the Beneficial Ownership Regulations*, or a majority owned subsidiary of such a company;
(b) a States trading company within the meaning of the States Trading Companies (Bailiwick of Guernsey) Law, 2001;
(c) a legal person controlled by the States of Alderney through ownership within the meaning of the Beneficial Ownership (Alderney) (Definition) Regulations, 2017 (or any successor regulations made under Section 25 of the Beneficial Ownership of Legal Persons (Alderney) Law, 2017; or
(d) a regulated person within the meaning of Section 41(2) of *the Beneficial Ownership Law*.

"**unique identifier**" means any unique combination of letters, numbers or symbols that refers to a specific natural person.

"**unique transaction identifier**" means any unique combination of letters, numbers or symbols that refers to a specific transaction. In respect of a *VASP* it also permits the traceability of the transaction from the *originator* to the beneficiary.

"**VASPs**" means virtual assets service providers.

"**vested interest**" means an interest which, whether or not currently in possession, is not contingent or conditional on the occurrence of any event.

"**virtual asset**" or "**VA**" means a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes, but virtual assets do not include digital representations of -

(a) fiat currencies; or
(b) general securities and derivatives within the meaning of category 2 in Schedule 1 to the *POI Law* and other financial assets.

"**voting rights**" means, in accordance with Regulation 7 of *the Beneficial Ownership Regulations*:

(1) a reference to the voting rights in a *relevant legal person* or other legal entity is to the rights conferred on shareholders in respect of their shares (or, in the case of an entity not

having a share capital, on members or officers) to vote at general meetings of the *relevant legal person* or other entity on all or substantially all matters.

(2) in relation to a *relevant legal person* or other legal entity that does not have general meetings at which matters are decided by the exercise of voting rights:

(a) a reference to exercising voting rights in the *relevant legal person* or other legal entity is to be read as a reference to exercising rights in relation to a person or entity that are equivalent to those of a person entitled to exercise voting rights in a company, and

(b) a reference to exercising more than 25% of the voting rights in the *relevant legal person* or legal entity is to be read as a reference to exercising the right under the constitution of the *relevant legal person* or entity to block changes to the overall policy of the entity or to the terms of its constitution.

(3) in applying this definition, the voting rights in a *relevant legal person* or other legal entity are to be reduced by any rights held by the person or entity itself.

"**wire transfer**" means any transaction carried out on behalf of a *payer* (both natural and legal) through a *financial services business* by electronic means with a view to making an amount of money available to a beneficiary person at another *financial services business*. The *payer* and the beneficiary may be the same person.

Appendix B

References

Legislation

The Relevant Enactments

Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999
http://www.guernseylegalresources.gg/article/97901/Criminal-Justice-Proceeds-of-Crime-Bailiwick-of-Guernsey-Law-1999-Consolidated-text

Drug Trafficking (Bailiwick of Guernsey) Law, 2000
http://www.guernseylegalresources.gg/article/97968/Drug-Trafficking-Bailiwick-of-Guernsey-Law-2000-Consolidated-text

Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011
http://www.guernseylegalresources.gg/article/99001/Terrorist-Asset-Freezing-Bailiwick-of-Guernsey-Law-2011-Consolidated-text

The Sanctions (Bailiwick of Guernsey) Law, 2018
https://www.guernseylegalresources.gg/laws/guernsey-bailiwick/s/sanctions/sanctions-bailiwick-of-guernsey-law-2018/

Terrorism and Crime (Bailiwick of Guernsey) Law, 2002
http://www.guernseylegalresources.gg/article/98997/Terrorism-and-Crime-Bailiwick-of-Guernsey-Law-2002-Consolidated-text

Disclosure (Bailiwick of Guernsey) Law, 2007
http://www.guernseylegalresources.gg/article/97922/Disclosure-Bailiwick-of-Guernsey-Law-2007-Consolidated-text

Transfer of Funds (Guernsey) Ordinance, 2017
http://www.guernseylegalresources.gg/article/160524/Transfer-of-Funds-Guernsey-Ordinance-2017

Transfer of Funds (Alderney) Ordinance, 2017
http://www.guernseylegalresources.gg/article/161322/Transfer-of-Funds-Alderney-Ordinance-2017

Transfer of Funds (Sark) Ordinance, 2017
http://www.guernseylegalresources.gg/article/160675/Transfer-Of-Funds-Sark-Ordinance-2017

Disclosure (Bailiwick of Guernsey) Regulations, 2007
https://www.gfsc.gg/sites/default/files/The-Disclosure-(BoG)-Reg-2007-as-amended.pdf

Terrorism and Crime (Bailiwick of Guernsey) Regulations, 2007
https://www.gfsc.gg/sites/default/files/The-Terrorism-and-Crime-(Bailiwick-of-Guernsey)-Regulations-2007-as-amended.pdf

Prescribed Business (Bailiwick of Guernsey) Law, 2008
http://www.guernseylegalresources.gg/article/117215/Prescribed-Businesses-Bailiwick-of-Guernsey-Law-2008-Consolidated-text

Beneficial Ownership of Legal Persons (Guernsey) Law, 2017
http://www.guernseylegalresources.gg/article/161719/Beneficial-Ownership-of-Legal-Persons-Guernsey-Law-2017-Consolidated-text

Beneficial Ownership of Legal Persons (Alderney) Law, 2017
https://www.guernseylegalresources.gg/laws/alderney/c/companies-and-commercial/beneficial-ownership-of-legal-persons-alderney-law-2017/

Beneficial Ownership (Definition) Regulations, 2017
http://www.guernseylegalresources.gg/article/161219/No-38---The-Beneficial-Ownership-Definition-Regulations-2017

Beneficial Ownership (Alderney) (Definitions) Regulations, 2017
http://www.guernseylegalresources.gg/article/162032/No-3---Beneficial-Ownership-Alderney-Definition-Regulations-2017

Beneficial Ownership of Legal Persons (Provision of Information) (Transitional Provisions) Regulations, 2017
http://www.guernseylegalresources.gg/article/162346/No-87---The-Beneficial-Ownership-of-Legal-Persons-Provision-of-Information-Transitional-Provisions-Regulations-2017

Beneficial Ownership of Legal Persons (Provision of Information) (Transitional Provisions) (Alderney) Regulations, 2017
http://www.guernseylegalresources.gg/article/163268/No-5---Beneficial-Ownership-of-Legal-Persons-Provision-of-Information-Transitional-Provisions-Alderney-Regulations-2017

Beneficial Ownership of Legal Persons (Nominee Relationships) Regulations, 2017
http://www.guernseylegalresources.gg/article/162878/No-102---The-Beneficial-Ownership-of-Legal-Persons-Nominee-Relationships-Regulations-2017

Beneficial Ownership of Legal Persons (Nominee Relationships) (Alderney) Ordinance, 2017
http://www.guernseylegalresources.gg/article/163273/Beneficial-Ownership-of-Legal-Persons-Nominee-Relationships-Alderney-Ordinance-2017

Beneficial Ownership of Legal Persons (Provision of Information) (Limited Partnerships) Regulations, 2017
http://www.guernseylegalresources.gg/article/163181/No-120---The-Beneficial-Ownership-of-Legal-Persons-Provision-of-Information-Limited-Partnerships-Regulation-2017

The Regulatory Laws

Banking Supervision (Bailiwick of Guernsey) Law, 2020
https://www.guernseylegalresources.gg/CHttpHandler.ashx?documentid=82857

Insurance Business (Bailiwick of Guernsey) Law, 2002
http://www.guernseylegalresources.gg/article/95374/Insurance-Business-Bailiwick-of-Guernsey-Law-2002-Consolidated-text

Insurance Managers and Insurance Intermediaries (Bailiwick of Guernsey) Law, 2002
http://www.guernseylegalresources.gg/article/95385/Insurance-Managers-and-Insurance-Intermediaries-Bailiwick-of-Guernsey-Law-2002-Consolidated-text

Protection of Investors (Bailiwick of Guernsey) Law, 2020
https://www.guernseylegalresources.gg/CHttpHandler.ashx?documentid=82884

Regulation of Fiduciaries, Administration Businesses and Company Directors, etc. (Bailiwick of Guernsey) Law, 2020
https://www.guernseylegalresources.gg/CHttpHandler.ashx?documentid=82886

The Lending, Credit and Finance (Bailiwick of Guernsey) Law, 2022
https://www.guernseylegalresources.gg/laws/guernsey-bailiwick/f/financial-services/lending-credit-and-finance-bailiwick-of-guernsey-law-2022-consolidated-text/

Other Relevant Legislation

Cash Controls (Bailiwick of Guernsey) Law, 2007
http://www.guernseylegalresources.gg/article/93998/Cash-Controls-Bailiwick-of-Guernsey-Law-2007-Consolidated-text

Cash Controls Law (Definition of Cash) (Bailiwick of Guernsey) Ordinance, 2009
http://www.guernseylegalresources.gg/article/93999/Cash-Controls-Law-Definition-of-Cash-Bailiwick-of-Guernsey-Ordinance-2009

Companies (Guernsey) Law, 2008
http://www.guernseylegalresources.gg/article/94138/Companies-Guernsey-Law-2008-Consolidated-text

Criminal Justice (Aiding and Abetting etc.) (Bailiwick of Guernsey) Law 2007
http://www.guernseylegalresources.gg/article/97848/Criminal-Justice-Aiding-and-Abetting-etc-Bailiwick-of-Guernsey-Law-2007-Consolidated-text

Criminal Justice (Attempts, Conspiracy and Jurisdiction) (Bailiwick of Guernsey) Law, 2006
https://www.guernseylegalresources.gg/laws/guernsey-bailiwick/c/crime-and-criminal-justice/others/criminal-justice-attempts-conspiracy-and-jurisdiction-bailiwick-of-guernsey-law-2006-consolidated-text/

Criminal Justice (Fraud Investigation) (Bailiwick of Guernsey) Law, 1991
http://www.guernseylegalresources.gg/article/97875/Criminal-Justice-Fraud-Investigation-Bailiwick-of-Guernsey-Law-1991-consolidated-text

Criminal Justice (International Co-operation) (Bailiwick of Guernsey) Law, 2001
http://www.guernseylegalresources.gg/article/97878/Criminal-Justice-International-Co-operation-Bailiwick-of-Guernsey-Law-2001

Criminal Justice (International Co-operation) (Enforcement of Overseas Forfeiture Orders) (Bailiwick of Guernsey) Ordinance, 2007
http://www.guernseylegalresources.gg/article/97882/Criminal-Justice-International-Co-operation-Enforcement-of-Overseas-Forfeiture-Orders-Bailiwick-of-Guernsey-Ordinance-2007-Consolidated-text

Criminal Justice (Miscellaneous Provisions) (Bailiwick of Guernsey) Law, 2006
https://www.guernseylegalresources.gg/laws/guernsey-bailiwick/c/crime-and-criminal-justice/others/criminal-justice-miscellaneous-provisions-bailiwick-of-guernsey-law-2006-consolidated-text/

Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) Ordinance, 2017
https://www.gov.gg/CHttpHandler.ashx?id=116261&p=0

Forfeiture of Money etc. in Civil Proceedings (Bailiwick of Guernsey) Law, 2007
http://www.guernseylegalresources.gg/article/98073/Forfeiture-of-Money-etc-in-Civil-Proceedings-Bailiwick-of-Guernsey-Law-2007-Consolidated-text

Forgery and Counterfeiting (Bailiwick of Guernsey) Law, 2006
https://www.guernseylegalresources.gg/laws/guernsey-bailiwick/c/crime-and-criminal-justice/others/forgery-and-counterfeiting-bailiwick-of-guernsey-law-2006-consolidated-text/

Fraud (Bailiwick of Guernsey) Law, 2009
https://www.guernseylegalresources.gg/laws/guernsey-bailiwick/c/crime-and-criminal-justice/others/fraud-bailiwick-of-guernsey-law-2009-consolidated-text/

Police Property and Forfeiture (Bailiwick of Guernsey) Law, 2006
https://www.guernseylegalresources.gg/laws/guernsey-bailiwick/p/police-prison-and-fire-services/police-property-and-forfeiture-bailiwick-of-guernsey-law-2006-consolidated-text/

Prevention of Corruption (Bailiwick of Guernsey) Law, 2003
https://www.guernseylegalresources.gg/laws/guernsey-bailiwick/c/crime-and-criminal-justice/others/prevention-of-corruption-bailiwick-of-guernsey-law-2003-consolidated-text/

Terrorism and Crime (Enforcement of Overseas Orders) (Bailiwick of Guernsey) Ordinance, 2007
http://www.guernseylegalresources.gg/article/98998/Terrorism-and-Crime-Enforcement-of-External-Orders-Bailiwick-of-Guernsey-Ordinance-2007

Guidance Links

European Guidelines

Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on Simplified and Enhanced Customer Due Diligence and the Factors Credit and Financial Institutions Should Consider when Assessing the Money Laundering and Terrorist Financing Risk Associated with Individual Business Relationships and Occasional Transactions
https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-on-risk-factors-and-simplified-and-enhanced-customer-due-diligence

Joint Guidelines under Article 25 of Regulation (EU) 2015/847 on the Measures Payment Service Providers Should Take to Detect Missing or Incomplete Information on the Payer or the Payee, and the Procedures they Should Put in Place to Manage a Transfer of Funds Lacking the Required Information
https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-to-prevent-transfers-of-funds-can-be-abused-for-ml-and-tf

Website Links

Bailiwick of Guernsey Websites

Guernsey Financial Services Commission
https://www.gfsc.gg/

Financial Intelligence Unit
http://www.guernseyfiu.gov.gg/

States of Guernsey
https://www.gov.gg/

States of Guernsey Sanctions
https://www.gov.gg/sanctions

Guernsey Registry
http://www.guernseyregistry.com/

Guernsey Registry Charities & NPOs Register
https://www.guernseyregistry.com/charities

We Are Guernsey (also known as Guernsey Finance)
https://www.weareguernsey.com/

Other Official Websites

Asia/Pacific Group on Money Laundering
http://www.apgml.org/

Basel Committee on Banking Supervision
http://www.bis.org/bcbs/index.htm

Caribbean Financial Action Task Force
https://www.cfatf-gafic.org/

Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures
https://www.coe.int/t/dghl/monitoring/moneyval/

Eastern and Southern Africa Anti-Money Laundering Group
http://www.esaamlg.org/

Egmont Group of Financial Intelligence Units
http://www.egmontgroup.org/

Eurasian Group on Combating Money Laundering and Financing of Terrorism
http://www.eurasiangroup.org/

European Parliament
http://www.europarl.europa.eu/portal/en

European External Action Service, with a link to the European Union Common Foreign and Security Policy
https://www.eeas.europa.eu/eeas/about-european-external-action-service_en#8424

Financial Action Task Force
http://www.fatf-gafi.org/

Financial Action Task Force of Latin America
http://www.gafilat.org/

Group of International Finance Centre Supervisors
https://www.groupgifcs.org/

Group of States against Corruption (Council of Europe)
http://www.coe.int/t/dghl/monitoring/greco/default_en.asp

Inter-Governmental Action Group against Money Laundering in West Africa
http://www.giaba.org/

International Association of Insurance Supervisors
http://www.iaisweb.org/home

International Forum of Sovereign Wealth Funds
http://www.ifswf.org/

International Monetary Fund
http://www.imf.org/external/index.htm

International Organization of Securities Commissions
http://www.iosco.org/

Interpol
https://www.interpol.int/

Isle of Man Financial Services Authority
http://www.iomfsa.im/

Jersey Financial Services Commission
http://www.jerseyfsc.org/

Middle East and North Africa Financial Action Task Force
http://www.menafatf.org/

Organisation for Economic Cooperation and Development
http://www.oecd.org/

Task Force on Money Laundering in Central Africa (*in French*)
http://spgabac.org/

Transparency International
https://www.transparency.org.uk/

UK Finance
https://www.ukfinance.org.uk/

United Kingdom Financial Conduct Authority
https://www.fca.org.uk/

United Kingdom Foreign, Commonwealth and Development Office
https://www.gov.uk/government/organisations/foreign-commonwealth-development-office

United Kingdom HM Treasury
https://www.gov.uk/government/organisations/hm-treasury

United Kingdom Joint Money Laundering Steering Group
http://www.jmlsg.org.uk/

United Kingdom Legislation
https://www.legislation.gov.uk/

United Kingdom National Crime Agency
http://www.nationalcrimeagency.gov.uk/

United Kingdom Office for Financial Sanctions Implementation
https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation

United Nations
http://www.un.org/en/index.html

United Nations Office on Drugs and Crime
http://www.unodc.org/

United Nations Security Council Sanctions Committee
https://www.un.org/sc/suborg/en/scsb

United States Department of State
https://www.state.gov/

United States Department of the Treasury
https://home.treasury.gov/

United States Office of Foreign Assets Control – Sanctions Programmes and Information
https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx

World Bank
http://www.worldbank.org/

World Customs Organization
http://www.wcoomd.org/en.aspx

Appendix C

Equivalent Jurisdictions

Australia	https://www.fatf-gafi.org/en/countries/detail/Australia.html
Austria	https://www.fatf-gafi.org/en/countries/detail/Austria.html
Belgium	https://www.fatf-gafi.org/en/countries/detail/Belgium.html
Bermuda	https://www.cfatf-gafic.org/member-countries/bermuda
Canada	https://www.fatf-gafi.org/en/countries/detail/Canada.html
Cyprus	https://www.coe.int/en/web/moneyval/jurisdictions/cyprus
Denmark	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Denmark.html
Estonia	https://www.coe.int/en/web/moneyval/jurisdictions/estonia
Finland	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Finland.html
France	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/france.html
Germany	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Germany.html
Gibraltar	https://www.coe.int/en/web/moneyval/jurisdictions/Gibraltar
Greece	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Greece.html
Hong Kong	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Hong-Kong-China.html
Hungary	https://www.coe.int/en/web/moneyval/jurisdictions/hungary
Ireland	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Ireland.html
Isle of Man	https://www.coe.int/en/web/moneyval/jurisdictions/isle_of_man
Italy	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Italy.html
Japan	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Japan.html
Jersey	https://www.coe.int/en/web/moneyval/jurisdictions/jersey
Latvia	https://www.coe.int/en/web/moneyval/jurisdictions/latvia
Liechtenstein	https://www.coe.int/en/web/moneyval/jurisdictions/liechtenstein
Lithuania	https://www.coe.int/en/web/moneyval/jurisdictions/lithuania
Luxembourg	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Luxembourg.html
Malta	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Malta.html
Netherlands	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/netherlands.html
New Zealand	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/New-Zealand.html
Norway	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Norway.html
Portugal	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Portugal.html
Singapore	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Singapore.html
Slovenia	https://www.coe.int/en/web/moneyval/jurisdictions/slovenia
Spain	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Spain.html
Sweden	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Sweden.html
Switzerland	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/Switzerland.html
United Kingdom	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/united-kingdom.html
United States of America	https://www.fatf-gafi.org/content/fatf-gafi/en/countries/detail/United-States.html

Appendix C to this *Handbook* was established to reflect those countries or territories which *the Commission* considers require regulated *FSBs*, and in limited circumstances *PBs*, to have in place standards to combat *ML* and *TF* consistent with *the FATF Recommendations* and where such businesses are appropriately supervised for compliance with those requirements. Appendix C is reviewed periodically with countries or territories being added or removed as appropriate.

The fact that a country or territory has requirements to combat *ML* and *TF* that are consistent with *the FATF Recommendations* means only that the necessary legislation and other means of ensuring compliance with *the FATF Recommendations* are in force in that country or territory. It does not provide assurance that a particular overseas business is subject to that legislation, or that it has implemented the necessary measures to ensure compliance with that legislation.

The firm is not obliged to deal with regulated *FSBs* in the jurisdictions listed above as if they were local, notwithstanding that they meet the requirements identified in this Appendix. The firm may, in deciding whether or not to deal with a regulated *FSB* or *PB*, impose higher standards than the minimum standards identified in this *Handbook* where it considers this necessary.

In accordance with the definition provided for in *Schedule 3*, an "**Appendix C business**" means –

(a) a *financial services business* supervised by *the Commission*; or

(b) a business which is carried on from –

(i) a country or territory listed in Appendix C to this *Handbook* which would, if it were carried on in *the Bailiwick*, be a *financial services business*; or

(ii) the United Kingdom, the Bailiwick of Jersey, *the Bailiwick* or the Isle of Man by a lawyer or an accountant;

and, in either case, is a business –

(A) which may only be carried on in that country or territory by a person regulated for that purpose under the law of that country or territory;

(B) the conduct of which is subject to requirements to forestall, prevent and detect *ML* and *TF* that are consistent with those in *the FATF Recommendations* in respect of such as business; and

(C) the conduct of which is supervised for compliance with the requirements referred to in subparagraph (B), by *the Commission* or an overseas regulatory authority.

The absence of a country or territory from the above list does not prevent the application of the introduced business provisions set out in Chapter 10 of this *Handbook*. In this respect the firm can still accept introduced business, provided the requirements in Section 10.6. of this *Handbook* are met.

Further information in respect of Appendix C and the treatment of an *Appendix C business* can be found in Section 9.6. of this *Handbook*.

Appendix D

Sector-Specific Risk Factors

Contents of this Appendix

1. This appendix provides sector-specific *risk* factors which the firm should consider when undertaking *business risk assessments* and *relationship risk assessments*.

2. This appendix should be read in conjunction with Chapter 3 to this *Handbook* and Paragraphs 2 and 3 of *Schedule 3* which detail the requirements in relation to the identification and management of risk, including the undertaking of *business risk assessments* and *relationship risk assessments*. Chapter 3 also provides more general *risk* factors which should be considered by firms across all sectors.

3. The *risk* factors described in Chapter 3 and this appendix are not exhaustive. The firm should take a holistic view of the *risk* associated with a *business relationship* or *occasional transaction* and note that isolated *risk* factors do not necessarily make a *business relationship* or *occasional transaction* high or low *risk* overall.

Retail Banking Sector

4. For the purpose of this *guidance*, retail banking means the provision of banking services to natural persons and small and medium-sized businesses. Examples of retail banking products and services include current *accounts*, mortgages, savings *accounts*, consumer and term loans and credit lines.

5. Due to the nature of the products and services offered, the relative ease of access and the often large volume of transactions and *business relationships*, retail banking is vulnerable to *TF, PF* and to all stages of the *ML* process. At the same time, the volume of *business relationships* and transactions associated with retail banking can make identifying *ML, TF* and *PF* associated with individual relationships and spotting suspicious transactions particularly challenging.

6. *Banks* should consider the following *risk* factors alongside those set out in Paragraph 3 of *Schedule 3* and Chapter 3 of this *Handbook*.

Product, Service and Transaction Risk Factors

7. The following factors may contribute to increasing *risk*:

   (a) the product's features favour anonymity.
   (b) the product allows payments from third parties that are neither associated with the product nor identified upfront, where such payments would not be expected (for example, for mortgages or loans).
   (c) the product places no restrictions on turnover, cross-border transactions or similar product features.
   (d) new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products where these are not yet well understood.
   (e) lending (including mortgages) secured against the value of assets in other jurisdictions, particularly countries where it is difficult to ascertain whether the *customer* has legitimate title to the collateral, or where the identities of parties guaranteeing the loan are hard to verify.
   (f) an unusually high volume or large value of transactions.

8. The following factors may contribute to reducing *risk*:

   (a) the product has limited functionality, for example in the case of:

      (i) a fixed term savings product with low savings thresholds;
      (ii) a product where the benefits cannot be realised for the benefit of a third party;

(iii) a product where the benefits are only realisable in the long term or for a specific purpose, such as retirement or a property purchase;
(iv) a low-value loan facility, including one that is conditional on the purchase of a specific consumer good or service; or
(v) a low-value product, including a lease, where the legal and beneficial title to the asset is not transferred to the *customer* until the contractual relationship is terminated or is never passed at all.

(b) the product can only be held by certain categories of *customers*, for example, pensioners, parents on behalf of their children, or minors until they reach the age of majority.
(c) transactions must be carried out through an *account* in the *customer's* name at an *Appendix C business*.
(d) there is no overpayment facility.

Customer Risk Factors

9. The following factors may contribute to increasing *risk*:

(a) the nature of the *customer*, for example:

(i) the *customer* is a cash-intensive undertaking.
(ii) the *customer* is an undertaking associated with higher levels of *ML risk*, for example, certain money remitters and gambling businesses.
(iii) the *customer* is an undertaking associated with a higher corruption risk, for example, operating in the extractive industries or the arms trade.
(iv) the *customer* is a charity or non-profit organisation that supports jurisdictions associated with an increased *TF risk.*
(v) the *customer* is a new undertaking without an adequate business profile or track record.
(vi) the *customer* is not resident within *the Bailiwick*.
(vii) the *customer's beneficial owner* cannot easily be identified, for example because the *customer's* ownership structure is unusual, unduly complex or opaque.

(b) the *customer's* behaviour, for example:

(i) the *customer* is reluctant to provide requested information or *identification data*, or appears deliberately to avoid face-to-face contact.
(ii) the *customer's* evidence of identity is in a non-standard form for no apparent reason.
(iii) the *customer's* behaviour or transaction volume is not in line with that expected from the category of *customer* to which they belong, or is unexpected based on the information the *customer* provided at *account* opening.
(iv) the *customer's* behaviour is unusual, for example, the *customer* unexpectedly and without reasonable explanation accelerates an agreed repayment schedule, by means either of lump sum repayments or early *termination*; deposits or demands pay-out of high-value bank notes without apparent reason; increases activity after a period of dormancy; or makes transactions that appear to have no economic rationale.

10. The following factor may contribute to reducing *risk*:

(a) the *customer* is a long-standing client whose previous transactions have not given rise to suspicion or concern, and the product or service sought is in line with the *customer's risk* profile.

Country or Geographical Risk Factors

11. The following factors may contribute to increasing *risk*:

    (a) the *customer's funds* are derived from personal or business links to jurisdictions associated with higher *ML, TF* and/or *PF risk*.
    (b) the payee is located in a jurisdiction associated with higher *ML, TF* and/or P*F risk*. In addition to those jurisdictions requiring a mandatory high risk rating by virtue of Paragraph 5(1)(c) of *Schedule 3*, the firm should pay particular attention to jurisdictions where groups committing terrorist offences are known to be operating, and jurisdictions subject to, or associated with, financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation.

12. The following factor may contribute to reducing *risk*:

    (a) countries associated with the transaction have an AML/CFT/CPF regime that is not less robust than that of *the Bailiwick* and are associated with low levels of predicate offences.

Distribution Channel Risk Factors

13. The following factors may contribute to increasing *risk*:

    (a) non-face-to-face *business relationships* or *occasional transactions*, where no adequate additional safeguards (for example, signatures in electronic form, electronic identification certificates and anti-impersonation fraud checks) are in place.
    (b) reliance on a third party's *CDD* measures in situations where the firm does not have a long-standing relationship with the referring third party.
    (c) new delivery channels that have not yet been tested.

14. The following factor may contribute to reducing *risk*:

    (a) the product is available only to *customers* who meet specific eligibility criteria set out by national public authorities, for example, benefit recipients or specific savings products for children within *the Bailiwick*.

Private Banking and Wealth Management Sector

15. Private banking is the provision of banking and other financial services to high-net-worth individuals and their families or businesses. It is also known as wealth management. *Customers* of private banking and wealth management firms can expect dedicated relationship management staff to provide tailored services covering, for example, banking (current accounts, mortgages and foreign exchange etc.), investment management and advice, fiduciary services, safe custody, insurance, family office services, tax and estate planning and associated facilities, including legal support.

16. Many of the features typically associated with private banking and wealth management, such as wealthy and influential *customers*; high-value transactions and portfolios; complex products and services, including tailored investment products; and an expectation of confidentiality and discretion are indicative of a higher *risk* for *ML* relative to those typically present in retail banking. Private banking and wealth management firms' services may be particularly vulnerable to abuse by *customers* who wish to conceal the origins of their *funds* or, for example, evade tax in their home jurisdiction.

17. Private banking and wealth management firms should consider the following *risk* factors alongside those set out in Paragraph 3 of *Schedule 3* and Chapter 3 of this *Handbook*.

Product, Service and Transaction Risk Factors

18. The following factors may contribute to increasing *risk*:

    (a) *customers* requesting large amounts of cash or other physical stores of value such as precious metals.
    (b) very high-value transactions.
    (c) financial arrangements involving jurisdictions associated with higher *ML*, *TF* and/or *PF risk*. The firm should pay particular attention to countries that have a culture of banking secrecy or that do not comply with international tax transparency standards.
    (d) lending (including mortgages) secured against the value of assets in other jurisdictions, particularly countries where it is difficult to ascertain whether the *customer* has legitimate title to the collateral, or where the identities of parties guaranteeing the loan are hard to verify.
    (e) the use of complex business structures such as trusts and private investment vehicles, particularly where the identity of the ultimate *beneficial owner* may be unclear.
    (f) business taking place across multiple countries, particularly where it involves multiple providers of financial services.
    (g) cross-border arrangements where assets are deposited or managed in another financial services business, either of the same financial group or outside of the group, particularly where the other *FSB* is based in a jurisdiction associated with higher *ML*, *TF* and/or *PF risk*. The firm should pay particular attention to jurisdictions with higher levels of predicate offences, a weak AML/CFT/CPF regime or weak tax transparency standards.

Customer Risk Factors

19. The following factors may contribute to increasing *risk*:

    (a) *customers* with income and/or wealth from high *risk* sectors such as arms, the extractive industries, construction, gambling or private military contractors.
    (b) *customers* about whom credible allegations of wrongdoing have been made.
    (c) *customers* who expect unusually high levels of confidentiality or discretion.
    (d) *customers* whose spending or transactional behaviour makes it difficult to establish 'normal', or expected patterns of behaviour.
    (e) very wealthy and influential *customers*, including *customers* with a high public profile and non-resident *customers*.
    (f) the *customer* requests that the firm facilitates the *customer* being provided with a product or service by a third party without a clear business or economic rationale.

Country or Geographical Risk Factors

20. The following factors may contribute to increasing *risk*:

    (a) business is conducted in countries that have a culture of banking secrecy or do not comply with international tax transparency standards.
    (b) the *customer* has a *relevant connection* to a jurisdiction associated with higher *ML*, *TF* and/or *PF risk*.

Money Service Provider Sector

21. Money service providers ("MSPs") include *banks* and firms that have been registered under Schedule 4 to *the Law* to operate a money services business (for example, a currency exchange) and cheque cashing; facilitate or transmit money or value through an informal money or value transfer system or network; or offer money broking or money changing services. The firms in this sector are diverse and range from individual businesses to international banking groups.

22. Some MSPs use agents to deliver payment services on their behalf. Agents often provide payment services as an ancillary component to their main business. Accordingly, their AML/CFT/CPF expertise may be limited.

23. The nature of the service provided can expose MSPs to *ML*, *TF* or *PF risk*. This is due to the simplicity and speed of transactions, their worldwide reach and their often cash-based character. Furthermore, the nature of this payment service means that MSPs often carry out *occasional transactions* rather than establishing *business relationships* with their *customers*, which means that their understanding of the *ML*, *TF* and *PF risk* associated with the *customer* may be limited.

24. MSPs should consider the following *risk* factors alongside those set out in Paragraph 3 of *Schedule 3* and Chapter 3 of this *Handbook*.

Product, Service and Transaction Risk Factors

25. The following factors may contribute to increasing *risk*:

    (a) the product allows high-value or unlimited-value transactions.
    (b) the product or service has a global reach.
    (c) the transaction is cash-based or funded with anonymous electronic money.
    (d) transfers are made from one or more payers in different countries to a payee's account in *the Bailiwick*.

26. The following factor may contribute to reducing *risk*:

    (a) the *funds* used in the transfer come from an *account* held in the *payer's* name at an *Appendix C business*.

Customer Risk Factors

27. The following factors may contribute to increasing *risk*:

    (a) the *customer's* business activity:

        (i) the *customer* owns or operates a business that handles large amounts of cash.
        (ii) the *customer's* business has a complicated ownership structure.

    (b) the *customer's* behaviour:

        (i) the *customer's* needs may be better serviced elsewhere, for example, because the MSP is not local to the *customer* or the *customer's* business.
        (ii) the *customer* appears to be acting for someone else, for example, others watch over the *customer* or are visible outside the place where the transaction is made, or the *customer* reads instructions from a note.
        (iii) the *customer's* behaviour makes no apparent economic sense, for example, the *customer* accepts a poor exchange rate or high charges unquestioningly, requests a transaction in a currency that is not official tender or commonly used in the jurisdiction where the *customer* and/or recipient is located or requests or provides large amounts of currency in either low or high denominations.
        (iv) the *customer's* transactions are always just below applicable thresholds, including the £10,000 threshold for *occasional transactions* set out in *Schedule 3* and the £1,000 threshold for *wire transfers* specified in *the Transfer of Funds Ordinance*.
        (v) the *customer's* use of the service is unusual, for example, they send or receive money to or from themselves or send *funds* on immediately after receiving them.

(vi) the *customer* appears to know little or is reluctant to provide information about the *payee*.
(vii) several of the firm's *customers* transfer *funds* to the same *payee* or appear to have the same identification information, for example, address or telephone number.
(viii) an incoming transaction is not accompanied by the required information on the *payer* or *payee*.
(ix) the amount sent or received is at odds with the *customer's* income (if known).

28. The following factors may contribute to reducing *risk*:

(a) the *customer* is a long-standing *customer* of the firm whose past behaviour has not given rise to suspicion and there are no indications that the *ML, TF* or *PF risk* might be increased.
(b) the amount transferred is low; however, the firm should note that low amounts alone will not be enough to discount *TF* or *PF risk.*

Country or Geographical Risk Factors

29. The following factors may contribute to increasing *risk*:

(a) the *payer* or the *payee* is located in a jurisdiction associated with higher *ML, TF* and/or *PF risk.*
(b) the *payee* is resident in a jurisdiction that has no, or a less developed, formal banking sector, which means that informal money remittance services, such as hawala, may be used at point of payment.

Distribution Channel Risk Factors

30. The following factors may contribute to increasing *risk*:

(a) there are no restrictions on the funding instrument, for example, cash, unrestricted E-money products, *wire transfers* or cheques.
(b) the distribution channel used provides a degree of anonymity.
(c) the service is provided entirely online without adequate safeguards.
(d) the money remittance service is provided through agents that:

(i) represent more than one principal;
(ii) have unusual turnover patterns compared with other agents in similar locations, for example, unusually high or low transaction sizes, unusually large cash transactions or a high number of transactions that fall just under the *CDD* threshold, or undertake business outside normal business hours;
(iii) undertake a large proportion of business with *payers* or *payees* from jurisdictions associated with higher *ML, TF* and/or *PF risk*;
(iv) appear to be unsure about, or inconsistent in, the application of group-wide AML//CFT/CPF policies; or
(v) are not from the financial sector and conduct another business as their main business.

(e) the money remittance service is provided through a large network of agents in different jurisdictions.
(f) the money remittance service is provided through an overly complex payment chain, for example, with a large number of intermediaries operating in different jurisdictions or allowing for untraceable (formal and informal) settlement systems.

31. The following factors may contribute to reducing *risk*:

(a) agents are themselves regulated *FSBs*.

(b) the service can be funded only by transfers from an account held in the *customer's* name at an *Appendix C business* or an *account* over which the *customer* can be shown to have control.

Investment Management Sector

32. Investment management is the management of an investor's assets to achieve specific investment goals. It includes both discretionary investment management, where investment managers take investment decisions on their *customers'* behalf, and advisory investment management, where investment managers advise their *customers* on which investments to make but do not execute transactions on their *customers'* behalf.

33. Investment managers usually have a limited number of private or institutional *customers* many of which are wealthy, for example, high-net-worth individuals, trusts, companies, government agencies and other investment vehicles. The *customers' funds* are often handled by a local custodian, rather than the investment manager. The *ML*, *TF* and *PF risk* associated with investment management is therefore driven primarily by the *risk* associated with the type of *customers* investment managers serve.

34. Investment management firms should consider the following *risk* factors alongside those set out in Paragraph 3 of *Schedule 3* and Chapter 3 of this *Handbook*.

Product, Service and Transaction Risk Factors

35. The following factors may contribute to increasing *risk*:

(a) transactions are unusually large.
(b) third party payments are possible.
(c) the product or service is used for subscriptions that are quickly followed by redemption possibilities, with limited intervention by the investment manager.

Customer Risk Factors

36. The following factors may contribute to increasing *risk*:

(a) the *customer's* behaviour, for example:

(i) the rationale for the investment lacks an obvious economic purpose.
(ii) the *customer* asks to repurchase or redeem a long-term investment within a short period after the initial investment or before the pay-out date without a clear rationale, in particular where this results in financial loss or payment of high transaction fees.
(iii) the *customer* requests the repeated purchase and sale of shares within a short period of time without an obvious strategy or economic rationale.
(iv) unwillingness to provide information or *identification data* on the *customer* and/or the *beneficial owner*.
(v) frequent changes to the identity information or payment details provided by the *customer* or *beneficial owner*.
(vi) the *customer* transfers *funds* in excess of those required for the investment and asks for surplus amounts to be reimbursed.
(vii) the circumstances in which the *customer* makes use of the 'cooling-off' period give rise to suspicion.
(viii) using multiple *accounts* without previous notification, especially when these *accounts* are held in multiple or high-*risk* jurisdictions.

(ix) the *customer* wishes to structure the relationship in such a way that multiple parties (for example, nominee companies) are used in different jurisdictions, particularly where these jurisdictions are associated with higher *ML, TF* and/or *PF risk.*

(b) the *customer's* nature, for example:

(i) the *customer* is a *legal person* or *legal arrangement* established in a jurisdiction associated with higher *ML, TF* and/or *PF risk*. The firm should pay particular attention to those jurisdictions that do not comply effectively with international tax transparency standards.
(ii) the *customer* is an investment vehicle that carries out little or no due diligence on its own clients.
(iii) the *customer* is an unregulated third party investment vehicle.
(iv) the *customer's* ownership and control structure is opaque.
(v) the *customer* or the *beneficial owner* holds a prominent position (other than a politically exposed position) that might enable them to abuse their position for private gain.
(vi) the *customer* is a non-regulated nominee company with unknown shareholders.

(c) the *customer's* business, for example, the *customer's funds* are derived from business in sectors that are associated with a high *risk* of financial crime.

37. The following factors may contribute to reducing *risk*:

(a) the *customer* is a government body from a country or territory listed in Appendix C to this *Handbook.*
(b) the *customer* is an institutional investor whose status has been verified by a government agency in a country or territory listed in Appendix C to this *Handbook*, for example, a government-approved pensions scheme.
(c) the *customer* is an *Appendix C business.*

Country or Geographical Risk Factors

38. The following factors may contribute to increasing *risk*:

(a) the investor or their custodian is based in a jurisdiction associated with higher *ML, TF* and/or *PF risk.*
(b) the *funds* come from a jurisdiction associated with higher *ML, TF* and/or *PF risk.*

Investment Fund Sector

39. The provision of CISs can involve multiple parties: the designated administrator, fund/principal manager, appointed advisers, the custodian/depositary and sub-custodians, registrars and, in some cases, prime brokers. Similarly, the distribution of these CISs can involve parties such as tied agents, advisory and discretionary wealth managers, platform service providers and independent financial advisers.

40. The type and number of parties involved in a CIS's distribution process depends on the nature of the CIS and may affect how much the *nominated firm* knows about the CIS' investors. In accordance with Section 4.6.1. of this *Handbook* the *nominated firm* retains responsibility for compliance with the AML/CFT/CPF obligations in respect of investors, although aspects of *CDD* measures may be carried out by one or more other parties subject to certain conditions.

41. CISs may be used by persons or entities for *ML, TF* and/or *PF* purposes:

(a) retail CISs are often distributed on a non-face-to-face basis; access to such CISs is often easy and relatively quick to achieve, and holdings in such funds can be transferred between different parties.
(b) alternative investment CISs, such as hedge funds, real estate and private equity funds, tend to have a smaller number of investors, which can be private individuals as well as institutional investors (pension funds, funds of funds). CISs that are designed for a limited number of high-net-worth individuals, or for family offices, can have an inherently higher *risk* of abuse for *ML, TF* and/or *PF* purposes than retail CISs, since investors are more likely to be in a position to exercise control over the CISs assets. If investors exercise control over the assets, such CISs are personal asset holding vehicles. Further detail in this regard can be found in Section 9.8.3.3. of this *Handbook.*
(c) notwithstanding the often medium to long-term nature of investments in CISs, which can contribute to limiting the attractiveness of these products for *ML* purposes, they may still appeal to money launderers on the basis of their ability to generate growth and income.

42. Other parties involved in the provision or distribution of a CIS (for example, intermediaries) may have to comply with their own *CDD* obligations and should also refer any other relevant guidance within this Appendix.

Product, Service and Transaction Risk Factors

43. The following factors may contribute to increasing the *risk* associated with the CIS:

(a) the CIS is designed for a limited number of high-net-worth individuals or family offices.
(b) it is possible to subscribe to the CIS and then quickly redeem the investment without the investor incurring significant administrative costs.
(c) units of or shares in the CIS can be traded without it or the *nominated firm* being notified at the time of the trade and, as a result, information about the investor is divided among several subjects (as is the case with CECISs traded on secondary markets).

44. The following factors may contribute to increasing the *risk* associated with the subscription:

(a) the subscription involves accounts or third parties in multiple jurisdictions, in particular where these jurisdictions are associated with a higher *ML, TF* and/or *PF risk.*
(b) the subscription involves third party subscribers or payees, in particular where this is unexpected.

45. The following factors may contribute to reducing the *risk* associated with the CIS:

(a) third party payments are not allowed.
(b) the CIS is open to small-scale investors only, with investments capped.

Customer Risk Factors

46. The following factors may contribute to increasing *risk*:

(a) the *customer's* behaviour is unusual, for example:

(i) the rationale for the investment lacks an obvious strategy or economic purpose or the *customer* makes investments that are inconsistent with the *customer's* overall financial situation, where this is known to the *nominated firm*.
(ii) the *customer* asks to repurchase or redeem an investment within a short period after the initial investment or before the pay-out date without a clear rationale, in particular where this results in financial loss or payment of high transaction fees.

(iii) the *customer* requests the repeated purchase and sale of shares within a short period of time without an obvious strategy or economic rationale.
(iv) the *customer* transfers *funds* in excess of those required for the investment and asks for surplus amounts to be reimbursed.
(v) the *customer* uses multiple *accounts* without previous notification, especially when these *accounts* are held in multiple jurisdictions or jurisdictions associated with higher *ML, TF* and/or *PF risk*.
(vi) the *customer* wishes to structure the relationship in such a way that multiple parties (for example, non-regulated nominee companies) are used in different jurisdictions, particularly where these jurisdictions are associated with higher *ML, TF* and/or *PF risk*.
(vii) the *customer* suddenly changes the settlement location without rationale, for example, by changing the *customer's* country of residence.
(viii) the *customer* and the *beneficial owner* are located in different jurisdictions and at least one of these jurisdictions is associated with higher *ML, TF* and/or *PF risk*.
(ix) the *beneficial owner's funds* have been generated in a jurisdiction associated with higher *ML, TF* and/or *PF risk*, in particular where the jurisdiction is associated with higher levels of predicate offences to *ML, TF* and/or *PF*.

47. The following factors may contribute to reducing *risk*:

(a) the *customer* is a government body from a country or territory listed in Appendix C to this *Handbook*.
(b) the *customer* is an institutional investor whose status has been verified by a government agency in a country or territory listed in Appendix C to this *Handbook*, for example, a government-approved pensions scheme.
(c) the *customer* is an *Appendix C business*.

Distribution Channel Risk Factors

48. The following factors may contribute to increasing *risk*:

(a) unclear or complex distribution channels that limit oversight of investments into a CIS and restrict the ability to monitor transactions, for example, the CIS uses a large number of sub-distributors for distribution outside of *the Bailiwick*.
(b) the distributor is located in a jurisdiction associated with higher *ML, TF* and/or *PF risk*.

49. The following factors may indicate lower *risk*:

(a) the CIS admits only a designated type of low-*risk* investor, such as *Appendix C businesses* investing as a principal (for example, life companies) or corporate pension schemes.
(b) the CIS can be purchased and redeemed only through an *Appendix C business*, for example a financial intermediary.

Country or Geographical Risk Factors

50. The following factors may contribute to increasing *risk*:

(a) investors' monies have been generated in jurisdictions associated with higher *ML, TF* and/or P*F risk*, in particular those associated with higher levels of predicate offences to *ML*.
(b) the CIS invests in sectors with higher corruption risk (for example, the extractive industries or the arms trade) in jurisdictions identified by credible sources as having significant levels of corruption or other predicate offences to *ML, TF* and/or *PF*, in particular where the CIS has a limited number of investors.

Life Insurance Sector

51. Life insurance products are designed to financially protect the policy holder against the risk of an uncertain future event, such as death, illness or outliving savings in retirement (longevity risk). The protection is achieved by an insurer who pools the financial risks that many different policy holders are faced with. Life insurance products can also be bought as investment products or for pension purposes.

52. Life insurance products are provided through different distribution channels to *customers* who may be natural or *legal persons* or *legal arrangements*. The beneficiary of the contract may be the policy holder or a nominated or designated third party; the beneficiary may also change during the term and the original beneficiary may never benefit.

53. Most life insurance products are designed for the long term and some will only pay out on a verifiable event, such as death or retirement. This means that many life insurance products are not sufficiently flexible to be the first vehicle of choice for money launderers. However, as with other financial services products, there is a *risk* that the *funds* used to purchase life insurance may be the proceeds of crime.

54. Firms in the life insurance sector should consider the following *risk* factors alongside those set out in Paragraph 3 of *Schedule 3* and Chapter 3 of this *Handbook*. Life insurance intermediaries may also find this guidance useful.

Product, Service and Transaction Risk Factors

55. The following factors may contribute to increasing *risk*:

    (a) flexibility of payments, for example, the product allows:

        (i) payments from unidentified third parties;
        (ii) high-value or unlimited-value premium payments, overpayments or large volumes of lower value premium payments; or
        (iii) cash payments.

    (b) ease of access to accumulated *funds*, for example, the product allows partial withdrawals or early surrender at any time, with limited charges or fees.
    (c) negotiability, for example, the product can be:

        (i) traded on a secondary market; or
        (ii) used as collateral for a loan.

    (d) anonymity, for example, the product facilitates or allows the anonymity of the *customer*.

56. Factors that may contribute to reducing *risk* include:

    (a) the product:

        (i) only pays out against a pre-defined event (for example, death) or on a specific date, such as in the case of credit life insurance policies covering consumer and mortgage loans and paying out only on death of the insured person;
        (ii) has no surrender value;
        (iii) has no investment element;
        (iv) has no third party payment facility;
        (v) requires that total investment is curtailed at a low value;
        (vi) is a life insurance policy where the premium is low;

(vii) only allows small-value regular premium payments, for example, no overpayment;
(viii) is accessible only through employers, for example, a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;
(ix) cannot be redeemed in the short or medium term, as in the case of pension schemes without an early surrender option;
(x) cannot be used as collateral;
(xi) does not allow cash payments; or
(xii) has conditions that must be met to benefit from tax relief.

Customer Risk Factors

57. The following factors may contribute to increasing *risk*:

(a) the nature of the *customer*, for example:

(i) *legal persons* whose structure makes it difficult to identify the *beneficial owner*;
(ii) the *customer's* age is unusual for the type of product sought (for example, the *customer* is very young or very old);
(iii) the contract does not match the *customer's* wealth situation;
(iv) the *customer's* profession or activities are regarded as particularly likely to be related to *ML*, for example, because they are known to be very cash intensive or exposed to a high risk of corruption;
(v) the contract is subscribed by a 'gatekeeper', such as a fiduciary company, acting on behalf of the *customer*; or
(vi) the policy holder and/or the beneficiary of the contract are companies with *nominee shareholders*.

(b) the *customer's* behaviour:

(i) in relation to the contract, for example:

a. the *customer* frequently transfers the contract to another insurer;
b. frequent and unexplained surrenders, especially when the refund is done to different *bank accounts*;
c. the *customer* makes frequent or unexpected use of 'free look' provisions/'cooling-off' periods, in particular where the refund is made to an apparently unrelated third party;
d. the *customer* incurs a high cost by seeking early *termination* of a product;
e. the *customer* transfers the contract to an apparently unrelated third party; or
f. the *customer's* request to change or increase the sum insured and/or the premium payment are unusual or excessive.

(ii) in relation to the beneficiary, for example:

a. the insurer is made aware of a change in beneficiary only when the claim is made;
b. the *customer* changes the beneficiary clause and nominates an apparently unrelated third party; or
c. the insurer, the *customer*, the *beneficial owner*, the beneficiary or the *beneficial owner* of the beneficiary are in different jurisdictions.

(iii) in relation to payments, for example:

a. the *customer* uses unusual payment methods, such as cash or structured monetary instruments or other forms of payment vehicles fostering anonymity;
b. payments from different *bank accounts* without explanation;
c. payments from *banks* that are not established in the *customer's* country of residence;
d. the *customer* makes frequent or high-value overpayments where this was not expected;
e. payments received from unrelated third parties; or
f. catch-up contribution to a retirement plan close to retirement date.

58. The following factors may contribute to reducing *risk*:

(a) in the case of corporate-owned life insurance, the *customer* is:

(i) an Appendix C business;
(ii) a public company listed on a stock exchange prescribed by *the Stock Exchange Regulations* or a majority owned subsidiary of such a company;
(iii) a public administration or a public enterprise from a country or territory listed in Appendix C to this *Handbook*.

Country or Geographical Risk Factors

59. The following factors may contribute to increasing *risk*:

(a) the insurer, the *customer*, the *beneficial owner*, the beneficiary or the *beneficial owner* of the beneficiary are based in, or connected with, jurisdictions associated with higher *ML, TF* and/or *PF risk*.
(b) premiums are paid through *accounts* held with *FSBs* established in jurisdictions associated with higher *ML, TF* and/or *PF risk.*
(c) the intermediary is based in, or connected with, jurisdictions associated with higher *ML, TF* and/or *PF risk*.

In all three cases the firm should pay particular attention to jurisdictions without effective AML/CFT/CPF supervision.

60. The following factors may contribute to reducing *risk*:

(a) countries are listed in Appendix C to this Handbook.
(b) countries are identified by credible sources as having a low level of corruption and other criminal activity.

Distribution Channel Risk Factors

61. The following factors may contribute to increasing *risk*:

(a) non-face-to-face sales, such as online, postal or telephone sales, without adequate safeguards, for example the use of signatures in electronic form or other controls such as those detailed in Section 6.5. of this *Handbook*;
(b) long chains of intermediaries;
(c) an intermediary is used in unusual circumstances (for example, unexplained geographical distance).

62. The following factors may contribute to reducing *risk*:

(a) an intermediary is well known to the insurer, who is satisfied that the intermediary applies CDD measures commensurate to the *risk* associated with the *business relationship* and in line with *the FATF Recommendations*.
(b) the product is only available to employees of certain companies that have a contract with the insurer to provide life insurance for their employees, for example, as part of a benefits package.

Legal Professional Sector

63. Internationally, there is a widely held perception that legal professionals will not report suspicions of *ML, TF* or *PF*, perhaps by making excessive use of LPP, or at a minimum that suspicious reports by legal professionals are only made where suspicion has become near certainty.

64. The Bailiwick's AML/CFT/CPF legislation contains a clear and specific requirement that a suspicious report is made in all circumstances where there is knowledge or suspicion, or reasonable grounds for having knowledge or suspicion, of *ML, TF* or *PF*. This reporting requirement is regardless of the value of the transaction or whether it involves tax matters.

65. Firms in the legal professional sector should consider the following *risk* factors alongside those set out in Paragraph 3 of *Schedule 3* and Chapter 3 of this *Handbook*.

Product, Service and Transaction Risk Factors

66. From a criminal's perspective putting illicit *funds* through a legal professional's client account can clean them, whether the *funds* are sent back to the *customer*, on to a third party, or invested in some way. In light of this, legal professionals should only use client accounts to hold funds for legitimate transactions for *customers*, or for another proper legal purpose. It can be difficult to draw a distinction between holding *customer funds* for a legitimate transaction and acting more like a *bank* but legal professionals should take care to not provide a de facto banking service for their *customers*.

67. The following factors may contribute to increasing *risk*:

(a) the instructions received from the *customer* are unusual in themselves, or they are unusual for the firm or the *customer*.
(b) the instructions or case change unexpectedly with no logical reason for the changes.
(c) funds are received from an unknown or unexpected third party.
(d) the *customer* requests payment (for example, the proceeds of a property sale) be made to an unknown, un-associated or obscure third party, including a private individual, whose identity is difficult or impossible to check.
(e) the *customer* deposits *funds* into the firm's client account prior to instructing the firm.
(f) the *customer* requests that *funds* received into the firm's client account are returned back to their source, to the *customer* or to an unknown or unconnected third party.
(g) the *customer* requests loss-making transactions which make no economic sense or where the loss is avoidable.
(h) the *customer's* instructions involve dealing with *funds* (for example, money or property) where the firm suspects that they are being transferred to avoid the attention of a trustee in a bankruptcy case or a law enforcement agency.

Customer Risk Factors

68. The following factors may contribute to increasing *risk*:

(a) the *customer* is excessively obstructive or secretive.

(b) where the *customer* is a charity or NPO, its purpose is unclear or unusually broad; the instructions appear unusual in the context of the charity or NPO's stated objectives; or the value of *funds* involved is unusual in the circumstances.

Accountancy Sector

69. Accountants perform a number of important functions in helping their *customers* organise and manage their financial affairs. These services may include the provision of advice to individuals and businesses in such matters as investment, company formation, trusts and other *legal arrangements*, as well as the optimisation of tax situations. Additionally, some may be directly involved in carrying out specific types of financial transactions (for example, holding or paying out *funds* relating to the purchase or sale of real estate) on behalf of *customers*.

70. Money launderers and those financing terrorism and proliferation need the same services as legitimate *customers*, including financial and business advice. Even unwitting involvement in *ML* can put the firm at *risk*.

71. To reduce this *risk*, firms in the accountancy sector should consider the following *risk* factors alongside those set out in Paragraph 3 of *Schedule 3* and Chapter 3 of this *Handbook*.

Product, Service and Transaction Risk Factors

72. The firm should be aware of the *risk* of the services it provides being used to assist in *ML, TF* or *PF*, including:

(a) advice provided by the firm on the setting up of *legal persons* or *legal arrangements* which may be used to obscure beneficial ownership or real economic purpose (including the setting up of trusts and companies, the change of name/corporate seat or other complex group structures).
(b) the misuse of introductory services, for example, to financial institutions.

Country or Geographical Risk Factors

73. The following factors may contribute to increasing *risk*:

(a) the firm's familiarity with a country or territory, including knowledge of local laws and regulations as well as the structure and extent of regulatory oversight.

Customer Risk Factors

74. The following factors may contribute to increasing *risk*:

(a) factors indicating that the *customer* is attempting to obscure the understanding of its business, ownership or the nature of its transactions, for example:

(i) the lack of a face-to-face introduction with the *customer*.
(ii) a subsequent lack of contact with the *customer* when this would normally be expected.
(iii) the beneficial ownership of the *customer* is unclear.
(iv) the position of intermediaries within the relationship is unclear.
(v) inexplicable changes in the ownership of the *customer*.
(vi) the activities of the *customer*, where it is a *legal person*, are unclear.
(vii) the legal structure of the *customer* has been altered numerous times (for example, name changes, transfers of ownership or changes of corporate seat).

(viii) management appear to be acting according to the instructions of unknown or inappropriate person(s).
(ix) the ownership structure of the *customer* is unnecessarily complex.

(b) factors indicating certain transactions, structures, geographical location, international activities or other factors which are not in keeping with the firm's understanding of the *customer's* business or economic situation, for example:

(i) *customer* instructions or *funds* outside of the *customer's* personal or business sector profile.
(ii) individual or classes of transactions that take place outside the established business profile for the *customer*, and expected activities and/or transactions is unclear.
(iii) employee numbers or structure are out of keeping with the size or nature of the *customer's* business (for example, the turnover of a company is unreasonably high considering the number of employees and assets used).
(iv) the *customer* starts or develops an enterprise with unexpected profile or early results.
(v) indications from the *customer* that they do not wish to obtain necessary governmental approvals/filings etc.
(vi) the *customer* offers to pay extraordinary fees for services which would not ordinarily warrant such a premium.

(c) *customer* industries, sectors or categories where opportunities for *ML*, *TF* or *PF* are particularly prevalent, for example:

(i) the *customer* has a high level of transactions in cash or readily transferable assets, among which illegitimate *funds* could be obscured.
(ii) investments in real estate at higher/lower prices than expected.
(iii) large international payments with no business rationale.
(iv) unusual financial transactions with unknown sources.
(v) the *customer* has multijurisdictional operations but does not have adequate centralised corporate oversight.

Estate Agency Sector

75. The growth of AML/CFT/CPF regulation and advances in technology have led to criminals using increasingly complex commercial arrangements that require the services of professionals outside of the financial services industry, including estate agents. For example, investment of illicit capital in property is a classic method of laundering. This investment is often made by way of chain transactions in property to disguise the source of funds.

76. Firms in the estate agency sector should consider the following *risk* factors alongside those set out in Paragraph 3 of *Schedule 3* and Chapter 3 of this *Handbook*.

Product, Service and Transaction Risk Factors

77. The following factors may contribute to increasing *risk*:

(a) the purchaser seeks to make large payments in cash, for example, when placing a deposit on a property.
(b) the purchaser deposits cash directly into the firm's client account at a *bank*.
(c) large payments are received from private *funds* other than the purchaser's, particularly where the purchaser has a low income.
(d) payments are received from one or more third parties with no prior or obvious connection to the purchaser.

(e) the purchaser makes an offer significantly above the asking price for a property with no obvious economic rationale.
(f) the *funds* for purchase are received from one party, with the beneficial ownership of the property assigned to a separate, unrelated party.
(g) the purchaser of a property seeks to sell the same property shortly after acquiring it.
(h) funds received from a purchaser are requested to be repaid to a third party where a property transaction, for whatever reason, does not take place.

Customer Risk Factors

78. The following factors may contribute to increasing *risk*:

(a) the *customer* makes an offer on a property prior to conducting a viewing, particularly where the *customer* has no prior connection to the property.
(b) the *customer* is unable, or unwilling, to explain the source of the *funds* being used to make a property purchase.
(c) the *customer's* finance arrangements appear unusual, for example, they do not involve a mortgage.
(d) the *customer* seeks to purchase a property using a complex structure of *legal persons* and/or *legal arrangements*, including nominee companies.

79. The following factors may contribute to reducing *risk*:

(a) the *customer* makes a property purchase in their own name using standard financing arrangements, for example, a combination of a deposit, mortgage and/or equity from a current property.

Appendix E

List of Domestic PEPs

Heads of State or Heads of Government Category

Guernsey

- Lieutenant-Governor

Alderney

- President of the States of Alderney

Senior Politicians and Other Important Officials of Political Parties

Guernsey[1]

- Members of the Policy & Resources Committee
- President of the Committee *for* Home Affairs
- President of the Committee *for* Health & Social Care
- President of the Committee *for the* Environment & Infrastructure
- President of the Committee *for* Employment & Social Security
- President of the Committee *for* Education, Sport & Culture
- President of the Committee *for* Economic Development
- President of the Development & Planning Authority
- President of the States' Trading Supervisory Board

Alderney

- Chairman of the Policy and Finance Committee
- Chairman of the General Services Committee
- Chairman of the Building and Development Control Committee
- Chairman of the Economic Development Committee

Sark

- Chairman of Policy and Finance Committee
- Chairman of Development Control

[1] https://gov.gg/deputies

Senior Government and Public Officials

Guernsey

- Head of the Public Service for the States of Guernsey

- Chief Strategy & Policy Officer
- Chief Operating Officer
- Chief Resources Officer

- States Treasurer
- Director of Planning
- Group Managing Director of the States' Trading Supervisory Board
- Registrar-General of Electors

- Head of Law Enforcement

- Commissioners of the Guernsey Financial Services Commission
- Director General of the Guernsey Financial Services Commission

- Registrar of Companies

- Data Protection Commissioner

- Director of Civil Aviation

- Chief Executive of the Channel Islands Competition & Regulatory Authorities

Alderney[2]

- Chief Executive of the States of Alderney
- States Treasurer

- Commissioners of the Alderney Gambling Control Commission
- Executive Director of the Alderney Gambling Control Commission

Sark[3]

- Speaker of Chief Pleas

- Senior Administrator
- Treasurer

[2] http://www.alderney.gov.gg/
[3] https://sarkgov.co.uk/contact-us

Senior Members of the Judiciary and Law Officers

Guernsey[4]

- Bailiff
- Deputy Bailiff

- Her Majesty's Procureur
- Her Majesty's Comptroller
- Her Majesty's Receiver General

- HM Greffier

Alderney

- Chairman of the Court of Alderney
- Clerk of the Court of Alderney

Sark

- Seneschal

Senior Executives of State Owned Body Corporates

Chairman, Chief Executive Officer and Finance Director (or equivalent) of:

- Guernsey Electricity Limited
- Guernsey Post Limited
- Aurigny Air Services Limited
- Jamesco 750 Limited

[4] http://guernseyroyalcourt.gg/article/3079/Court-Officials

Appendix F

Introducer Certificate

Name of Accepting Business:	
Name of Introducer:	
Account Name (in full):	
Details of Associated Account/s (which are part of the same structure):	

Introducer's Contact Details	
Address:	
Telephone:	
Fax:	
E-mail:	

The Introducer certifies that it is an Appendix C business and in respect of this account it has obtained and holds identification data equivalent to that required to satisfy the Handbook on Countering Financial Crime (AML/CFT/CPF) ("the Handbook") issued by the Guernsey Financial Services Commission, as updated from time to time.

The information disclosed for this account by the Introducer accurately reflects the information held and is being given for account opening and maintenance purposes only. The Introducer undertakes to keep the accepting business apprised of any changes to the information contained within this certificate and to supply certified copies or originals of the identification data upon request without delay.

Signature: _____ _____

Full Name: _____ _____

Official Position: _____ _____

Date: _____ _____

Please indicate the number of supplementary pages being submitted: IC2 ☐ IC3 ☐ IC4 ☐

Introducer Certificate IC2

Identification Information

Name of Introducer: _____

Account Name (in full): _____

1. To be completed for applicants for business who are individuals or partners in a partnership only.
(Please complete Sections 1 and 3 below and attach additional copies of this sheet (IC2) as required)

	1		2	
Full name:				
Any other name(s) used (including former names, e.g. maiden name):				
Nationality: (including all nationalities held)				
Date and place of birth:				
Occupation (including name of any employer where applicable)				
Current residential address (including postcode): *A PO Box only address is insufficient*				
Does the Introducer consider the individual to be, or to be associated with, a PEP?	Yes ☐	No ☐	Yes ☐	No ☐
Jurisdiction(s) and/or international organisations associated with any political function or connection				

2. To be completed for applications for business who are companies, partnerships, trusts or foundations.
(Please complete Sections 2 and 3 below and attach additional copies of this sheet (IC2) as required)

Date of incorporation/ registration/ settlement:	
Registration number: (if applicable)	
Place of incorporation/ registration: (if applicable)	
Current registered office address/ or address of trustees:	
Date of establishment: (if unincorporated/unregistered)	
Legal jurisdiction: (if unincorporated/unregistered)	
Type of trust/ foundation/ company:	

Is it a trading entity?		Does it have bearer shares or bearer warrants?		Does it have nominee shareholders?	
Yes ☐	No ☐	Yes ☐	No ☐	Yes ☐	No ☐

3. To be completed for all applicants for business.

Nature of activities or purpose and intended nature of business relationship or occasional transaction: (please provide a full description)	
For all foreign PEP relationships and high risk relationships: Source of any funds and source of the wealth of the customer and any beneficial owner who is a PEP[1]: (including the period over which this has been derived)	
Account activity:	

[1] At the discretion of the accepting business it may be appropriate for information on the source of any funds and the source of wealth to be provided for relationships other than high risk or relationships domestic PEPs or international organisation PEPs.

Introducer Certificate IC3

Related Parties

Name of Introducer: _____

Account Name (in full): _____

Details of all principal(s) (see IC5 for definition) including beneficial owners[1] and excluding officers of the Introducer. (Please complete the section below and attach additional copies of this sheet as required)

	No.		No.	
Full name:				
Any other name(s) used (including former names, e.g. maiden name):				
Nationality: (including all nationalities held)				
Date and place of birth:				
Occupation (including name of any employer)				
Current residential address (including postcode) *Note: A PO Box only address is insufficient*				
Role of principal and date relationship commenced.				
Does the Introducer consider the individual to be, or to be associated with, a PEP?	Yes ☐	No ☐	Yes ☐	No ☐
Jurisdiction(s) and/or international organisations associated with any political function or connection				

	No.		No.	
Full name				
Any other name(s) used (including former names, e.g. maiden name):				
Nationality: (including all nationalities held)				
Date and place of birth				
Occupation (including name of any employer)				
Current residential address (including postcode) *Note: A PO Box only address is insufficient*				
Role of principal and date relationship commenced.				
Does the Introducer consider the individual to be, or to be associated with, a PEP?	Yes ☐	No ☐	Yes ☐	No ☐
Jurisdiction(s) and/or international organisations associated with any political function or connection				

[1] Other than the beneficial owners of a corporate trustee which is licensed by the Commission.

Introducer Certificate IC4

Additional Information

Name of Introducer: _____

Account Name (in full): _____

This section is to be used by the specified business to identify any additional information or documentation that it requires over and above the stated minimum and/or for the Introducer to provide additional information to supplement the details contained in IC1, IC2 and/or IC3.

Introducer Certificate IC5

Notes and Guidance

These notes and the definitions below are intended to assist the Introducer in completing the required forms and to enable greater consistency to be achieved.

Term	Definition
Associated accounts	Refers to an account with the same specified business where any of the principals are connected with an account in the same group or structure.
Account activity	An estimate of the total flow of funds in and out of the account should be provided. An estimate of the expected maximum account turnover should also be provided. For a trading operation, the scale and volume of transactions should be explained.
Bearer shares	Where bearer shares are subsequently issued (after the opening of the account) such that the "Yes" box needs ticking in IC2, an updated form should be supplied to the accepting specified business without delay.
Certified copy	An officer or authorised signatory of a regulated financial services business will be an acceptable certifier. An acceptable 'certified copy' document should be an accurate and complete copy of the original such that the certifier will sign and date the copy document printing his position, capacity and company name.
Government issued personal identification number	Includes government issued personal identification number, for example a social security/ national insurance number, or other government issued unique identifier, for example a passport or driving licence number.
Handbook	The Handbook on Countering Financial Crime (AML/CFT/CPF) issued by the Guernsey Financial Services Commission, as updated from time to time.
Introducer	Is an Appendix C business (see definition in the Handbook).
Nature of activities or purpose and intended nature of business relationship	A sufficient description should be provided to enable the accepting specified business to properly categorise the underlying nature of the arrangements. If the activity is of a commercial nature, then additional information may be required.
PEP	A Politically exposed person, and includes such a person within the Bailiwick (domestic PEP) or any other jurisdiction ("foreign PEP"), as well as a person appointed with a prominent function by an international organisation. Further details about each can be found within Chapter 8 of the Handbook. The jurisdiction(s) associated with an individual's political exposure, either by a position held or any connection with a PEP, should also be provided.
Principal	Includes any person or other entity that has or is likely to receive a benefit in the foreseeable future or who the Introducer customarily treats as having an economic interest.
Role	This might include, for example, a beneficial owner, a shareholder, beneficiary, settlor, partner, etc.
Signatory	The General Introducer Certificate will need to be signed or initialled (where appropriate) in line with the Introducer's current mandate/authorised signatory list held with the accepting specified business.
Source of wealth	The origins of the wealth of the customer and any beneficial owner who is a PEP (and over what period) should be identified. Generally, simple one word answers will be unacceptable, for example, 'income', 'dividends', 'Bill Smith', or 'work'. A brief description to give a fuller picture is expected, for example, 'sale of UK private company in 1997', 'life time savings of settler who was a doctor', 'inheritance from parents' UK estate' and 'UK property development over the last 10 years'.
Specified business	A financial services business or a prescribed business in the Bailiwick of Guernsey.
Trading	Implies commercial activity which may include a business, invoicing or re-invoicing operations. For clarity, a 'trading company' does not include a personal service/employment company.

Please refer to the accepting specified business should you have any doubt or queries about completing this Introducer Certificate.

Appendix G

Schedule 3 to the Law

[SCHEDULE 3

SPECIFIED BUSINESSES

ARRANGEMENT OF PARAGRAPHS

PROVISIONS APPLICABLE TO TRUSTEES AND PARTNERS

PART IV
DESIGNATION OF SUPERVISORY AUTHORITY

PART V
MISCELLANEOUS

[SCHEDULE 3

SPECIFIED BUSINESSES

PART I

INTRODUCTORY PROVISIONS AND RISK ASSESSMENT

Application.

1. (1) Subject to [subparagraphs (2) and (3)], this Schedule applies to any business that is a financial services business or a prescribed business; and a business to which this Schedule applies is referred to in this Schedule as a specified business.

(2) [Save in the case of a business of the type described in paragraph 6 of Schedule 2, this Schedule] does not apply to a prescribed business where –

(a) the total turnover of the person carrying on the prescribed business in respect of the prescribed business does not exceed £50,000 per annum,

(b) the prescribed business –

(i) if it is an estate agent, does not hold deposits, or

(ii) if it is a prescribed business other than an estate agent, does not carry out occasional transactions,

(c) the services of the prescribed business are provided only to customers or clients resident in the Bailiwick, and

(d) the funds received by the prescribed business are drawn on a bank operating from or within the Bailiwick.

[(3) Paragraphs 2, 3, 10, and 15 of this Schedule do not apply to a business of the type described in paragraph 6 of Schedule 2, but an individual carrying on by way of business the activities described in paragraph 6 of Schedule 2 who is under an obligation to register with the Commission under paragraph 2 of Schedule 5 must have regard to –

(a) any relevant rules and guidance in the Handbook,

(b) any relevant notice or instruction issued by the Commission under this Law, and

(c) the NRA,

in understanding, for the purposes of this Schedule, its money laundering and terrorist financing risks, and determining, for the purposes of this Schedule, what constitute appropriate measures to manage and mitigate risks, and what constitutes a low or high risk business relationship.]

General duty to understand, and assess and mitigate, risks.

2. A specified business must –

(a) understand its money laundering and terrorist financing risks, and

(b) have in place effective policies, procedures and controls to –

(i) identify,

(ii) assess,

(iii) mitigate,

(iv) manage, and

(v) review and monitor,

those risks in a way that is consistent with the requirements of this Schedule, the relevant enactments, the requirements of the Handbook, and the NRA; and this Schedule shall be construed consistently with this duty.

Duty to carry out risk assessments.

3. (1) Without prejudice to the generality of the duty under paragraph 2, a specified business must –

(a) carry out and document a suitable and sufficient money laundering business risk assessment, and a suitable and sufficient terrorist financing business risk assessment, which are specific to the specified business, and

(b) regularly review its business risk assessments, at a minimum annually and more frequently when changes to the business of the specified business occur, so as to keep them up to date and, where, as a result of that review, changes to the business risk assessments are required, it must make those changes.

(2) In carrying out its business risk assessments under subparagraph (1) the business must consider all relevant risk factors before determining –

(a) the level of overall risk to the business,

(b) the type and extent of the risks that the business is willing to accept in order to achieve its strategic objectives (its **"risk appetite"**), and

(c) the appropriate level and type of mitigation to be applied.

(3) The business risk assessments must be appropriate to the nature, size and complexity of the business, and be in respect of –

(a) customers, and the beneficial owners of customers,

(b) countries and geographic areas, and

(c) products, services, transactions and delivery channels (as appropriate), and in particular in respect of the money laundering or terrorist financing risks that may arise in relation to –

(i) the development of new products and new business practices, before such products are made available and such practices adopted, and

(ii) the use of new or developing technologies for both new and pre-existing products, before such technologies are used and adopted[,]

[and the business risk assessments must include (without limitation) consideration of the implications for, and risks to, the business of the offences specified in the NRA as being the most likely predicate offences of the Bailiwick being used for money laundering or terrorist financing.]

(4) A specified business must –

(a) prior to the establishment of a business relationship or the carrying out of an occasional transaction, undertake a risk assessment of that proposed business relationship or occasional transaction, and

(b) regularly review any risk assessment carried out under subparagraph (a) so as to keep it up to date and, where changes to that risk assessment are required, it must make those changes.

(5) When undertaking a risk assessment under subparagraph (4)(a) or reviewing a risk assessment under subparagraph (4)(b), a specified business must –

(a) take into account its risk appetite and risk factors relating to the type or types of customer (and the beneficial owners of the customer), country or geographic area, and product, service, transaction and delivery channel that are relevant to the business relationship or occasional transaction in question, and

(b) understand that such risk factors, and any other risk factors, either singly or in combination, may increase or decrease the potential risk posed by the business relationship or occasional transaction.

(6) A specified business must –

(a) have in place policies, procedures and controls approved by its board that are appropriate and effective, having regard to the assessed risk, to enable it to mitigate and manage –

(i) risks identified in the business risk assessments and in risk assessments undertaken under subparagraph 4(a), and

(ii) risks relevant, or potentially relevant, to the business identified in the NRA (which risks must be incorporated into the business risk assessments),

(b) regularly review and monitor the implementation of those policies, controls and procedures, and enhance them if such enhancement is necessary or desirable for the mitigation and management of those risks, and

(c) take additional measures to manage and mitigate higher risks identified in the business risk assessments and in risk assessments undertaken under subparagraph 4(a).

(7) A specified business must have regard to –

(a) any relevant rules and guidance in the Handbook,

(b) any relevant notice or instruction issued by the Commission under this Law, and

(c) the NRA,

in determining, for the purposes of this Schedule, what constitutes a high or low risk, what its risk appetite is, and what constitute appropriate measures to manage and mitigate risks.

(8) A specified business must comply with subparagraphs (1)(a) and (6)(a) –

(a) as soon as reasonably practicable after 31st March 2019, or

(b) in the case of a specified business which only becomes such on or after 31st March 2019, as soon as reasonably practicable after it becomes such a business,

and subparagraphs (a) and (b) shall be construed consistently with the provisions of the Handbook.

(9) Without prejudice to subparagraph (8), until a specified business has complied with subparagraph (6)(a) it must continue to maintain the policies, procedures and controls it was required to establish and maintain under the FSB Regulations and the PB Regulations.

PART II

CUSTOMER DUE DILIGENCE ETC.

Customer due diligence.

4. (1) A specified business shall, subject to the following provisions of this Schedule, ensure that the steps in subparagraph (3) are carried out –

(a) when carrying out the activities in subparagraphs (2)(a) and (b) and in the circumstances in subparagraphs (2)(c) and (d), and

(b) in relation to a business relationship established prior to the coming into force of this Schedule –

(i) in respect of which there is maintained an anonymous account or an account in a fictitious name, as soon as possible after the coming into force of this Schedule and in any event before such account is used again in any way, and

(ii) where it does not fall within subparagraph (i) and to the extent that such steps have not already been carried out, at appropriate times on a risk-sensitive basis.

(2) The activities and circumstances referred to in subparagraph (1) are –

(a) establishing a business relationship,

(b) carrying out an occasional transaction,

(c) where the specified business knows or suspects or has reasonable grounds for knowing or suspecting –

(i) that, notwithstanding any exemptions or thresholds pursuant to this Schedule, any party to a business relationship is engaged in money laundering or terrorist financing, or

(ii) that it is carrying out a transaction on behalf of a person, including a beneficial owner, who is engaged in money laundering or terrorist financing, and

(d) where the specified business has doubts about the veracity or adequacy of previously obtained identification data.

(3) The steps referred to in subparagraph (1) are that –

(a) the customer shall be identified and the identity of the customer verified using identification data,

(b) any person purporting to act on behalf of the customer shall be identified and that person's identity and authority to so act shall be verified,

(c) the beneficial owner shall be identified and reasonable measures shall be taken to verify such identity using identification data and such measures shall include, in the case of a customer which is a legal person or legal arrangement, [measures to understand the nature of the customer's business and its ownership and control structure,]

(d) a determination shall be made as to whether the customer is acting on behalf of another person and, if the customer is so acting, reasonable measures shall be taken to identify that other person and to obtain sufficient identification data to verify the identity of that other person,

(e) the purpose and intended nature of each business relationship and occasional transaction shall be understood, and information shall be obtained as appropriate to support this understanding, and

(f) a determination shall be made as to whether the customer or beneficial owner is a politically exposed person, and, if so, whether he or she is a foreign politically exposed person, a domestic politically exposed person or a person who is or has been entrusted with a prominent function by an international organisation.

(4) A specified business is not required to identify any shareholder or beneficial owner in relation to –

(a) a customer, and

(b) a person which ultimately controls a customer,

that is a company listed on a recognised stock exchange within the meaning of the Beneficial Ownership (Definition) Regulations, 2017[ze], or a majority owned subsidiary of such a company.

(5) Where a specified business –

---

ze G.S.I. No. 38 of 2017; as amended by G.S.I. No. 51 of 2017; G.S.I. No. 99 of 2017; and G.S.I. No. 121 of 2017.

(a) forms a suspicion of money laundering or terrorist financing by a customer or other person, and

(b) reasonably believes that carrying out the steps in subparagraph (3), paragraph 5(3) or paragraph 11 would tip off that customer or person,

it shall not carry out those steps, but shall instead make a disclosure pursuant to Part I of the Disclosure Law, or section 15 or 15A, or section 12 (as appropriate) of the Terrorism Law.

(6) For the avoidance of doubt, a specified business must not treat a business relationship or occasional transaction as low risk for all money laundering and terrorist financing purposes solely because the business relationship or occasional transaction was assessed to be low risk.

[(7) A specified business must have regard to any relevant rules and guidance in the Handbook in determining, for the purposes of subparagraph (3)(c) and paragraphs 5(3)(a)(iii) and 5(3)(a)(v)(D), what constitutes reasonable measures.]

Enhanced customer due diligence.

5. (1) Where a specified business is required to carry out customer due diligence, it must also carry out enhanced customer due diligence in relation to high risk business relationships and occasional transactions, including, without limitation –

(a) a business relationship or occasional transaction in which the customer or any beneficial owner is a foreign politically exposed person,

(b) where the specified business is a financial services business, a business relationship which is –

(i) a correspondent banking relationship, or

(ii) similar to such a relationship in that it involves the provision of services, which themselves amount to financial services business or facilitate the carrying on of such business, by one financial services business to another,

(c) a business relationship or an occasional transaction –

(i) where the customer or beneficial owner has a relevant connection with a country or territory that –

A. provides funding or support for terrorist activities, or does not apply (or insufficiently applies) the Financial Action Task Force Recommendations, or

B. is a country otherwise identified by the Financial Action Task Force as a country for which such measures are appropriate,

(ii) which the specified business considers to be a high risk relationship, taking into account any notices, instructions or warnings issued from time to time by the Commission and having regard to the NRA,

(d) a business relationship or an occasional transaction which has been assessed as a high risk relationship, and

(e) a business relationship or an occasional transaction in which the customer, the beneficial owner of the customer, or any other legal person in the ownership or control structure of the customer, is a legal person that has bearer shares or bearer warrants.

(2) A specified business must also carry out enhanced measures in relation to business relationships and occasional transactions, whether otherwise high risk or not, which involve or are in relation to –

(a) a customer who is not resident in the Bailiwick,

(b) the provision of private banking services,

(c) a customer which is a legal person or legal arrangement used for personal asset holding purposes, or

(d) a customer which is –

(i) a legal person with nominee shareholders, or

(ii) owned by a legal person with nominee shareholders.

(3) In subparagraphs (1) and (2) –

(a) **"enhanced customer due diligence"** means –

(i) obtaining senior management approval for establishing a business relationship or undertaking an occasional transaction,

[(ii) obtaining senior management approval for, in the case of either –

A. an existing business relationship with a foreign politically exposed person, or

B. an existing high risk business relationship with a domestic politically exposed person or a person

who is a politically exposed person by virtue of subparagraph (4)(b),

continuing that relationship,]

(ii) obtaining senior management approval for, in the case of an existing business relationship with a foreign politically exposed person, continuing that relationship,

(iii) taking reasonable measures to establish and understand the source of any funds and of the wealth of –

(A) the customer, and

(B) the beneficial owner, where the beneficial owner is a politically exposed person,

(iv) carrying out more frequent and more extensive ongoing monitoring, including increasing the number and timing of controls applied and selecting patterns of activity or transactions that need further examination, in accordance with paragraph 11, and

(v) taking one or more of the following steps as would be appropriate to the particular business relationship or occasional transaction –

(A) obtaining additional information about the customer, such as the type, volume and value of the customer's assets and additional information about the customer's beneficial owners,

(B) verifying additional aspects of the customer’s identity,

(C) obtaining additional information to understand the purpose and intended nature of each business relationship and occasional transaction, and

(D) taking reasonable measures to establish and understand the source of wealth of beneficial owners not falling within subparagraph (iii), and

(b) **"enhanced measures"** means the carrying out of appropriate and adequate enhanced measures in relation to a business relationship or occasional transaction, to mitigate and manage the specific higher risk of money laundering and terrorist financing resulting from the matters listed in subparagraph (2) that are relevant to that relationship or transaction.

(4) [Subject to subparagraphs (5) and (5A)], in this Schedule **"politically exposed person"** means –

(a) a natural person who has, or has had at any time, a prominent public function, or who has been elected or appointed to such a function, including, without limitation –

(i) heads of state or heads of government,

(ii) senior politicians and other important officials of political parties,

(iii) senior government officials,

(iv) senior members of the judiciary,

(v) senior military officers, and

(vi) senior executives of state owned body corporates,

(and such a person shall be referred to as a **"foreign politically exposed person"** unless he or she holds or has held or has been elected or appointed to the prominent public function in question in respect of the Bailiwick, in which case he or she shall be referred to as a **"domestic politically exposed person"**),

(b) a person who is, or who has been at any time, entrusted with a prominent function by an international organisation,

(c) an immediate family member of a person referred to in (a) or (b) including, without limitation, a spouse, partner, parent, child, sibling, parent-in-law or grandchild of such a person and in this subparagraph **"partner"** means a person who is considered by the law of the country or territory in which the relevant public function is held as being equivalent to a spouse, or

(d) a [close associate of a person referred to in (a) or (b)], including, without limitation –

(i) a person who is widely known to maintain a close business relationship with such a person, or

(ii) a person who is in a position to conduct substantial financial transactions on behalf of such a person.

(5) A specified business may treat a domestic politically exposed person as not being a politically exposed person five years after the person ceased to be entrusted with a public function if the senior management of the business has documented that the business is satisfied that –

(a) it understands the source of the funds within the business relationship or occasional transaction, and

(b) there is no reason to continue to treat the person as a politically exposed person.

[(5A) A person is not a politically exposed person for the purposes of this Schedule if that person –

(a) was not a politically exposed person within the meaning of regulation 5(2)(b) of the FSB Regulations or regulation 5(2)(b) of the PB Regulations, when those Regulations were in force, and

(b) ceased to be entrusted with a prominent public function in respect of the Bailiwick before 31st March 2019.]

(6) Subject to subparagraph (9), a specified business may treat a person falling within subparagraph (4)(b) as not being a politically exposed person seven years after the person ceased to be entrusted with a prominent function by an international organisation if the senior management of the business has documented that the business is satisfied that –

(a) it understands the source of the funds within the business relationship or occasional transaction, and

(b) there is no reason to continue to treat the person as a politically exposed person.

(7) Subject to subparagraph (9), a specified business may treat any other politically exposed person as not being a politically exposed person for the purposes of this Schedule seven years after the person ceased to be entrusted with a public function if the senior management of the business has documented that the business is satisfied that –

(a) it has established and understands the source of the person's wealth, and that of the funds within the business relationship or occasional transaction, and

(b) there is no reason to continue to treat the person as a politically exposed person.

(8) Subparagraphs (5) to (7) apply in respect of persons falling within subparagraphs (4)(c) and (d) (immediate family members and close associates) in respect of the person in question as they do in respect of that person.

(9) Subparagraphs (6) and (7) do not apply in respect of a head of state or a head of government, a head of an international organisation, a person with the power to direct the spending of significant sums, or persons falling within subparagraphs (4)(c) and (d) in respect of such persons.

(10) For the purposes of subparagraph 1(c), a customer or beneficial owner has a **"relevant connection"** with a country or territory if the customer or beneficial owner –

(a) is the government, or a public authority, of the country or territory,

(b) is a politically exposed person within the meaning of subparagraph (4) in respect of the country or territory,

(c) is resident in the country or territory,

(d) has a business address in the country or territory,

(e) derives funds from –

(i) assets held by the customer or beneficial owner, or on behalf of the customer or beneficial owner, in the country or territory, or

(ii) income arising in the country or territory, or

(f) has any other connection with the country or territory which the specified business considers, in light of that business' duties under this Schedule (including but not limited to its duties under paragraph 2), to be a relevant connection for those purposes.

(11) A specified business must have regard to any relevant rules and guidance in the Handbook in determining –

(a) for the purposes of subparagraph (1), what constitute high risk business relationships and occasional transactions, and

(b) for the purposes of subparagraphs (5) to (7), if there is a reason to continue to treat the person mentioned there as a politically exposed person.

Customer due diligence for low risk relationships.

6. [(1) Where a specified business is required to carry out customer due diligence in relation to a business relationship or occasional transaction which –

(a) has been assessed as a low risk relationship pursuant to paragraph 3(4)(a) or in accordance with the NRA, or

(b) in the case of a business of the type described in paragraph 6 of Schedule 2, is a relationship of a type specified in the Handbook for the purposes of this paragraph,

the business or individual (as the case may be) may, subject to the following provisions of this paragraph, apply reduced or simplified customer due diligence measures.]

(2) The discretion in subparagraph (1) may only be exercised –

(a) in accordance with the requirements set out in the Handbook, and

[(b) where paragraph 3 applies to a specified business, by a specified

business that complies with the requirements of that paragraph.]

(3) For the avoidance of doubt, the discretion in subparagraph (1) shall not be exercised –

(a) where the specified business forms a suspicion that any party to a business relationship or occasional transaction or any beneficial owner is or has been engaged in money laundering or terrorist financing, or

(b) in relation to business relationships or occasional transactions where the risk is other than low.

Timing of identification and verification.

7. (1) Identification and verification of the identity of any person or legal arrangement pursuant to paragraphs 4 to 6 must, subject to subparagraph (2) and paragraph 4(1)(b), be carried out before or during the course of establishing a business relationship or before carrying out an occasional transaction.

(2) Verification of the identity of the customer and any of the beneficial owners may be completed following the establishment of a business relationship provided that to do so would be consistent with the risk assessment of the business relationship conducted pursuant to paragraph 3(4)(a), and –

(a) the verification is completed as soon as reasonably practicable thereafter,

(b) the need to do so is essential not to interrupt the normal conduct of business, and

(c) appropriate and effective policies, procedures and controls are in place which operate so as to manage risk, including, without limitation, a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed or the

monitoring of large or complex transactions [being carried out outside] the expected norms for that business relationship.

[(3) In the case of a business of the type described in paragraph 6 of Schedule 2, subparagraph (2) is modified to apply as if –

(a) the words "to do so would be consistent with the risk assessment of the business relationship conducted pursuant to paragraph 3(4)(a), and" were deleted, and

(b) for item (c) there were substituted the following item –

"(c) any relevant rules and guidance in the Handbook are complied with.".]

Accounts and shell banks.

8. (1) A specified business must, in relation to all customers –

(a) not set up or keep anonymous accounts or accounts in fictitious names, and

(b) maintain accounts in a manner which facilitates the meeting of the requirements of this Schedule, and the relevant rules and guidance in the Handbook.

(2) A specified business must –

(a) not enter into, or continue, a correspondent banking relationship with a shell bank, and

(b) take appropriate measures to ensure that it does not enter into, or continue, a correspondent banking relationship where the respondent bank is known to permit its accounts to be used by a shell bank.

(3) In this paragraph –

(a) **"consolidated supervision"** means supervision by a regulatory authority of all aspects of the business of a group of bodies corporate carried on worldwide, to ensure compliance with –

(i) the Financial Action Task Force Recommendations, and

(ii) other international requirements,

and in accordance with the Core Principles of Effective Banking Supervision issued by the Basel Committee on Banking Supervision as revised or reissued from time to time,

(b) **"physical presence"** means the presence of persons involved in a meaningful way in the running and management of the bank which, for the avoidance of doubt, is not satisfied by the presence of a local agent or junior staff, and

(c) **"shell bank"** means a bank that has no physical presence in the country or territory in which it is incorporated and licensed and which is not a member of a group of bodies corporate which is subject to effective consolidated supervision.

Non-compliance with customer due diligence measures etc.

9. Where a specified business can not comply with any of paragraph [4(3)(a) to (e)] or paragraph 11(1)(a) to (b) it must –

(a) in the case of an existing business relationship, terminate that business relationship,

(b) in the case of a proposed business relationship or occasional transaction, not enter into that business relationship or carry out that occasional transaction with the customer, and

(c) consider whether a disclosure must be made pursuant to Part I of the Disclosure Law, or section 15 or 15A, or section 12 (as appropriate) of the Terrorism Law.

Introduced business.

10. (1) In the circumstances set out in subparagraph (2), a specified business may accept a written confirmation of identity and other matters from an introducer in relation to the requirements of paragraph 4(3)(a) to (e) provided that –

(a) the specified business also requires copies of identification data and any other relevant documentation on the identity of the customer and beneficial owner to be made available by the introducer to the specified business immediately upon request, and

(b) the introducer keeps such identification data and documents.

(2) The circumstances referred to in subparagraph (1) are that the introducer –

(a) is an Appendix C business, or

(b) is either an overseas branch office of, or a member of the same group of legal persons or legal arrangements as, the specified business with which it is entering into the business relationship (**"receiving specified business"**), and –

(i) the ultimate legal person or legal arrangement of the group of legal persons or legal arrangements of which

both the introducer and the receiving specified business are members, falls within subparagraph (a), and

(ii) the conduct of the introducer is subject to requirements to forestall, prevent and detect money laundering and terrorist financing (including the application of any appropriate additional measures to effectively handle the risk of money laundering or terrorist financing) that are consistent with those in the Financial Action Task Force Recommendations in respect of such a business (particularly Recommendations 10, 11 and 12), and the introducer has implemented a programme to combat money laundering and terrorist financing that is consistent with the requirements of Recommendation 18, and

(iii) the conduct both of the introducer, and of the group of legal persons or legal arrangements of which both the introducer and the receiving specified business are members, is supervised or monitored for compliance with the requirements referred to in subparagraph (ii), by the Commission or [a relevant supervisory authority].

(3) Notwithstanding subparagraph (1), where reliance is placed upon the introducer the responsibility for complying with the relevant provisions of paragraph 4 remains with the receiving specified business.

PART III
ENSURING COMPLIANCE AND RECORD KEEPING

Monitoring transactions and other activity.

11. (1) A specified business shall perform ongoing and effective monitoring of any business relationship, which shall include –

(a) reviewing identification data and records to ensure they are kept up to date, accurate and relevant, and updating such data and records when they are not up to date, accurate or relevant,

(b) scrutinising any transactions or other activity to ensure that the transactions are consistent with the [specified] business' knowledge of the customer, their business and risk profile (including, where necessary, the sources of funds) and paying particular attention to all –

(i) complex transactions,

(ii) transactions which are both large and unusual, and

(iii) unusual patterns of activity or transactions,

which have no apparent economic purpose or no apparent lawful purpose, and

(c) ensuring that the way in which identification data is recorded and stored is such as to facilitate the ongoing monitoring of each business relationship.

(2) The extent of any monitoring carried out under this paragraph and the frequency at which it is carried out shall be determined on the basis of materiality and risk including, without limitation, whether or not the business relationship is a high risk relationship.

(3) Without prejudice to the generality of paragraph (2), where within an existing business relationship there are complex and unusually large transactions, or unusual patterns of transactions, which have no apparent economic or lawful purpose, a specified business shall –

(a) examine the background and purpose of those transactions, and

(b) increase the degree and nature of monitoring of the business relationship.

Reporting suspicion.

12. (1) Subject to subsection (2), a specified business shall –

(a) appoint a person of at least [manager level] as the Money Laundering Reporting Officer, provide the name, title and email address of that person to the Commission as soon as is reasonably practicable and, in any event, within fourteen days starting from the date of that person's appointment, and ensure that all employees are aware of the name of that person,

(b) if it is a financial services business which comprises more than one individual, nominate a person to –

(i) receive disclosures, under Part I of the Disclosure Law and section 15 of the Terrorism Law (a **"nominated officer"**), in the absence of the Money Laundering Reporting Officer, and

(ii) otherwise carry out the functions of the Money Laundering Reporting Officer in that officer's absence,

and ensure that all employees are aware of the name of that nominated officer,

(c) if it is a prescribed business which comprises more than one individual, nominate a person to –

(i) receive disclosures, under Part I of the Disclosure Law and section 12 of the Terrorism Law (a **"nominated**

officer"), in the absence of the Money Laundering Reporting Officer, and

(ii) otherwise carry out the functions of the Money Laundering Reporting Officer in that officer's absence,

and ensure that all employees are aware of the name of that nominated officer,

(d) provide the name, title and email address of the Money Laundering Reporting Officer appointed under (a), and of any person nominated under (b) or (c), to the [Financial Intelligence Unit] as soon as is reasonably practicable and, in any event, within fourteen days starting from the date of that person's appointment or nomination (as the case may be),

(e) ensure that where an employee, other than the Money Laundering Reporting Officer, is required to make a disclosure under Part I of the Disclosure Law, or section 15 or section 12 (as appropriate) of the Terrorism Law, that this is done by way of a report to the Money Laundering Reporting Officer, or, in that officer's absence, to a nominated officer,

(f) ensure that the Money Laundering Reporting Officer, or in that officer's absence a nominated officer, in determining whether or not he or she is required to make a disclosure under Part I of the Disclosure Law, or section 15A or section 12 (as appropriate) of the Terrorism Law, takes into account all relevant information,

(g) ensure that the Money Laundering Reporting Officer, or, in his or her absence, a nominated officer, is given prompt access to any other information which may be of assistance to him or her in considering any report, and

(h) ensure that it establishes and maintains such other appropriate and effective procedures and controls as are necessary to ensure compliance with requirements to make disclosures under Part I of the Disclosure Law, and sections 15 and 15A or section 12 (as appropriate) of the Terrorism Law.

(2) A person who, immediately prior to the coming into force of this Schedule (**"Commencement"**), was a money laundering reporting officer of a financial services business or a prescribed business, having been appointed as such under Part III of the FSB Regulations or Part III of the PB Regulations, as the case may be, shall be deemed to have been appointed as that business' Money Laundering Reporting Officer under subparagraph (1)(a) on Commencement, for the purposes of this Schedule.

(3) A person who, immediately prior to Commencement, was a nominated officer of a financial services business or a prescribed business, having been nominated as such under Part III of the FSB Regulations or Part III of the PB Regulations, as the case may be, shall be deemed to have been nominated as that business' nominated officer under subparagraph (1)(a) on Commencement, for the purposes of this Schedule.

(4) The requirement at subparagraph (1)(a) to provide the name, title and email address of the Money Laundering Reporting Officer to the Commission, and the requirements at subparagraph (1)(d), do not apply in respect of a person [deemed to have been appointed] or nominated under subparagraph (2) or (3) (as the case may be).

[(5) In the case of a business of the type described in paragraph 6 of Schedule 2, this paragraph is modified to apply as if for the whole paragraph there were substituted –

" **12.** In the case of a specified business of the type described in paragraph 6 of Schedule 2, the individual concerned (**"P"**) shall ensure that –

(a) in determining whether P is required to make a disclosure under Part I of the Disclosure Law, and sections 15 and 15A or section 12 (as appropriate) of the Terrorism Law, P takes into account all relevant information, and

(b) P establishes and maintains appropriate and effective procedures as are necessary to ensure compliance with requirements to make disclosures under Part I of the Disclosure Law, and sections 15 and 15A or section 12 (as appropriate) of the Terrorism Law.".]

Employee screening and training.

13. (1) A specified business shall maintain appropriate and effective procedures, proportionate to the nature and size of the business and to its risks, when hiring employees or admitting any person as a partner in the business, for the purpose of ensuring high standards of employee and partner probity and competence.

(2) [Subject to subparagraph (2A),] a specified business shall ensure that relevant employees, and any partners in the business, receive comprehensive ongoing training (at a frequency which has regard to the money laundering and terrorist financing risks to the business) in –

(a) the relevant enactments, this Schedule and the Handbook,

(b) the personal obligations of employees, and partners, and their potential criminal liability under this Schedule and the relevant enactments,

(c) the implications of non-compliance by employees, and partners, with any rules, guidance, instructions, notices or other similar instruments made for the purposes of this Schedule, and

(d) its policies, procedures and controls for the purposes of forestalling, preventing and detecting money laundering and terrorist financing.

[(2A) In the case of a specified business of the type described in paragraph 6 of Schedule 2, the individual concerned ("**P**") shall, having regard to the money laundering

and terrorist financing risks to the company or companies of which P is a director, maintain an understanding of the relevant enactments, this Schedule (including any guidance, instructions, notices or other similar instruments issued or made under this Schedule) and the Handbook, and of P's obligations thereunder.]

(3) A specified business shall identify relevant employees and partners in the business who, in view of their particular responsibilities, should receive additional and ongoing training, appropriate to their roles, in the matters set out in subparagraph (2) and must provide such additional training.

Record-keeping.

14. (1) Subject to the provisions of this paragraph, a specified business must keep a comprehensive record of each transaction with a customer or an introducer, including the amounts and types of currency involved in the transaction (if any); and such a record shall be referred to as a **"transaction document"**.

(2) A specified business shall keep –

(a) all transaction documents, risk assessments undertaken under paragraph 3(4), and any customer due diligence information, or

(b) copies thereof,

for the minimum retention period.

(3) A specified business must keep copies of business risk assessments carried out under paragraph 3(1) until the expiry of the period of five years starting from the date on which they cease to be operative.

(4) Where a specified business is required by any enactment, rule of law or court order to provide a transaction document or any customer due diligence information to any person before the end of the minimum retention period, the specified business shall –

(a) keep a copy of the transaction document or customer due diligence information until the period has ended or the original is returned, whichever occurs first, and

(b) maintain a register of transaction documents and customer due diligence information so provided.

(5) A specified business shall also keep records of –

(a) any reports made to a reporting officer as referred to in paragraph 12 and of any disclosure made under Part I of the Disclosure Law, or section 15 or 15A, or section 12 (as appropriate), of the Terrorism Law made other than by way of a report to the reporting officer, for five years starting from –

(i) in the case of a report or a disclosure in relation to a business relationship, the date the business relationship ceased,

(ii) in the case of a report or a disclosure in relation to an occasional transaction, the date that transaction was completed, or

(iii) in any other case, the event in respect of which the report or disclosure was made,

(b) any training carried out under paragraph 13 for five years starting from the date the training was carried out,

(c) any minutes or other documents prepared pursuant to paragraph 15(1)(c) until –

(i) the expiry of a period of five years starting from the date they were finalised, or

(ii) they are superseded by later minutes or other documents prepared under that paragraph,

whichever occurs later, and

(d) its policies, procedures and controls which it is required to establish and maintain pursuant to this Schedule, until the expiry of a period of five years starting from the date that they ceased to be operative.

(6) Documents and customer due diligence information, including any copies thereof, kept under this paragraph –

(a) may be kept in any manner or form, provided that they are readily retrievable, and

(b) must be made available promptly –

(i) to an auditor, and

(ii) to any police officer, the [Financial Intelligence Unit], the Commission or any other person, where such documents or customer due diligence information are requested pursuant to this Schedule or any relevant enactment.

[(7) In the case of a business of the type described in paragraph 6 of Schedule 2, this paragraph is modified to apply as if –

(a) in subparagraph (2)(a), ", risk assessments undertaken under paragraph 3(4)," were deleted, and

(b) subparagraphs (3), (5)(b), (c) and (d) were deleted.]

Ensuring compliance, corporate responsibility and related requirements.

15. (1) A specified business must, in addition to complying with the preceding requirements of this Schedule –

(a) if it is a specified business which comprises more than one individual, appoint a person of at least [manager level] as the Money Laundering Compliance Officer and provide the name, title and email address of that person to the Commission as soon as is reasonably practicable and, in any event, within fourteen days starting from the date of that person's appointment,

(b) establish such other policies, procedures and controls as may be appropriate and effective (having regard to the risk of money laundering and terrorist financing and the size of the business) for the purposes of forestalling, preventing and detecting money laundering and terrorist financing,

[(ba) without prejudice to the generality of subparagraph (b), establish an independent audit function (where appropriate, having regard to the money laundering and terrorist financing risks, and the size and nature, of the specified business in question), for the purpose of evaluating the adequacy and effectiveness of the policies, procedures and controls adopted by the specified business to comply with the requirements of this Schedule, the relevant enactments and the Handbook,]

(c) establish and maintain an effective policy, for which responsibility must be taken by the board, for the review of its compliance with the requirements of this Schedule and the Handbook, and such policy shall include provision as to the extent and frequency of such reviews,

(d) ensure that a review of its compliance with this Schedule and the Handbook is discussed and minuted at a meeting of the board at

appropriate intervals, and in considering what is appropriate a specified business must have regard to the risk taking into account –

(i) the size, nature and complexity of the specified business,

(ii) its customers, products and services, and

(iii) the ways in which it provides those products and services,

(e) subject to subparagraph (2) ensure that any of its branch offices and, where it is a body corporate, any body corporate of which it is the majority shareholder or control of which it otherwise exercises, which, in either case, is a specified business in any country or territory outside the Bailiwick (together, for the purposes of this paragraph, its "**subsidiaries**"), complies there with –

(i) the requirements of this Schedule and the Handbook, and

(ii) any requirements under the law applicable in that country or territory which are consistent with the Financial Action Task Force Recommendations,

provided that, where requirements under subparagraphs (i) and (ii) differ, a specified business must ensure that the requirement which provides the highest standard of compliance, by reference to the Financial Action Task Force Recommendations, is complied with,

(f) subject to subparagraph (2), ensure that it and its subsidiaries effectively implement policies, procedures and controls in respect of the sharing of information (including but not limited

to customer, account and transaction information) between themselves for the purposes of –

(i) carrying out customer due diligence,

(ii) sharing suspicions relating to money laundering and terrorist financing that have been formed and reported to the [Financial Intelligence Unit] (unless the [Financial Intelligence Unit] has instructed that they should not be so shared), and

(iii) otherwise forestalling, preventing and detecting money laundering and terrorist financing,

whilst ensuring that such policies, procedures and controls protect the confidentiality of such information, and

(g) where it is a specified business to which Schedule 4 applies, ensure that the conduct of any agent that it uses is subject to requirements to forestall, prevent and detect money laundering and terrorist financing that are consistent with those in the Financial Action Task Force Recommendations in respect of such an agent.

(2) The obligations under subparagraphs (1)(e) and (f) apply to the extent that the law of the relevant country or territory allows and if the law of the [country] or territory does not so allow in relation to any requirement of this Schedule, the specified business must notify the Commission accordingly.

[PART IIIA

SPECIFIC PROVISIONS ABOUT VIRTUAL ASSETS

Purpose of this Part.

15A. This Part of this Schedule makes provision in respect of the transfer of virtual

assets.

Expressions used in this Part.

15B. In this Part of this Schedule –

"appropriate authorities" means the Commission, His Majesty's Procureur, the salaried police force of the Island of Guernsey, the Guernsey Border Agency, the Director of the Economic and Financial Crime Bureau, the Financial Intelligence Unit, the Director of the Revenue Service, the Policy and Resources Committee (when acting under any enactment in respect of international sanctions measures) or any other Bailiwick of Guernsey person, authority, body or agency specified for the purposes of this Part of this Schedule in the Handbook,

"batch transfer" means a transfer comprised of a number of individual virtual asset transfers from one or more originators that are being sent to the same VASP, but may or may not be ultimately intended for different persons,

"beneficiary" means the person or legal arrangement who is identified by the originator as the receiver of the requested transfer of the virtual asset,

"beneficiary information" means information, or information of a class or description, specified for the purposes of this Part of this Schedule in requirements set out in the Handbook,

"beneficiary VASP" means the VASP which receives the transfer of the virtual asset from the originating VASP directly or through an intermediary VASP and makes the virtual asset available to the beneficiary,

"intermediary VASP" means a VASP which it is not acting on behalf of the originator or beneficiary but receives or transmits a virtual asset on behalf of the originating VASP, the beneficiary VASP or another intermediary VASP,

"originating VASP" means the VASP which initiates the transfer of the virtual asset and transfers the virtual asset upon receiving the order for a transfer of the virtual

asset from or on behalf of the originator,

"originator" means the customer who allows the transfer of the virtual asset from the customer's account or, where there is no account, the person who places the order with the originating VASP to perform the transfer,

"originator information" means information, or information of a class or description, specified for the purposes of this Part of this Schedule in requirements set out in the Handbook,

"transfer" of a virtual asset means a transaction carried out on behalf of an originator through an originating VASP by electronic means with a view to making a virtual asset available to a beneficiary at a beneficiary VASP, irrespective of whether the originator and the beneficiary are the same person,

"unique transaction identifier" means a combination of letters, numbers or symbols determined by the VASP which permits the traceability of the transaction from the originator to the beneficiary,

"VASPs" and **"virtual assets"** have the meanings respectively given in section 90(1) of the Lending, Credit and Finance (Bailiwick of Guernsey) Law, 2022.

Originator and beneficiary information – duties of VASPs.

15C. (1) An originating VASP must, in respect of any virtual asset transfer –

(a) obtain and hold required and accurate originator information and required beneficiary information,

(b) ensure that the information specified in (a) accompanies the transfer of the virtual asset to the beneficiary VASP immediately and securely,

(c) make the information specified in (a) available on request to the Commission and other appropriate authorities as soon as is reasonably practicable,

(d) not execute any virtual asset transfer in respect of which (b) is not complied with, and

(e) in the case of a transaction which would be an occasional transaction but for the sum involved being [under £1,000], obtain and hold such information, or information of such class or description, as may be specified for the purposes of this Part of this Schedule in requirements set out in the Handbook.

(2) A beneficiary VASP must, in respect of any virtual asset transfer –

(a) obtain and hold required and accurate beneficiary information and required originator information,

(b) make the information specified in (a) available on request to the Commission and other appropriate authorities as soon as is reasonably practicable, and

(c) in the case of a transaction which would be an occasional transaction but for the sum involved being [under £1,000], obtain and hold such information, or information of such class or description, as may be specified for the purposes of this Part of this Schedule in requirements set out in the Handbook.

(3) An intermediary VASP must, in respect of any virtual asset transfer –

(a) take reasonable measures which are consistent with straight-through processing to identify transfers received by it that are not accompanied by the originator and beneficiary information specified in (1)(a),

(b) without prejudice to the obligations to make disclosure imposed on specified businesses by paragraph 4(5), report to the Commission repeated failures by an originating VASP, beneficiary VASP or intermediary VASP to comply with the requirements of this Schedule as to the obtaining, holding, verification, retention, provision and use of information in respect of virtual asset transfers,

(c) ensure that any beneficiary information and originator information accompanying the transfer is retained with it,

(d) subject to (e), ensure that the information specified in (c) accompanies the onward transfer that the intermediary VASP will be making,

(e) where technical limitations prevent the information specified in (c) from accompanying an onward transfer, keep a comprehensive record of all information received from the originating VASP or another intermediary VASP for a period of not less than five years starting from the date of receipt of the virtual asset by the intermediary VASP, and

(f) have risk-based policies for –

(i) determining when to reject, suspend or otherwise refuse to execute virtual asset transfers because of information deficiencies, and

(ii) the taking of appropriate follow-up action.

Further obligations on beneficiary VASPs.

15D. Beneficiary VASPs must, without prejudice to the provisions of paragraph 15C –

(a) before making a virtual asset available to a beneficiary –

(i) monitor the completeness of the originator information, and

(ii) take remedial action where the information specified in (i) is incomplete,

(b) have risk-based policies for –

(i) determining when to reject, suspend or otherwise refuse to execute virtual asset transfers because of information deficiencies, and

(ii) the taking of appropriate follow-up action, and

(c) without prejudice to the obligations to make disclosure imposed on specified businesses by paragraph 4(5), report to the Commission repeated failures by an originating VASP, beneficiary VASP or intermediary VASP to comply with the requirements of this Schedule as to the obtaining, holding, verification, retention, provision and use of information in respect of virtual asset transfers.

Batch transfers.

15E. In the case of a batch transfer, and without prejudice to the provisions of paragraph 15C, an originating VASP must –

(a) ensure that the batch file contains required and accurate originator information and required beneficiary information,

(b) ensure that the information specified in (a) is such as to permit the traceability within the beneficiary jurisdiction of each

transaction comprised in the batch from the originator to the beneficiary, and

(c) include the originator's account number or unique transaction identifier and/or such other information, or information of such class or description, as may be specified for the purposes of this Part of this Schedule in requirements set out in the Handbook,

and **"beneficiary jurisdiction"** in (b) means the jurisdiction in which the beneficiary VASP receives the transfer of the virtual assets in question.

No cross-border requirement for transfers, etc.

15F. For the avoidance of doubt, the provisions of this Schedule apply in respect of a transfer of virtual assets irrespective of whether the transfer or other service or activity –

(a) is a cross-border transaction, or

(b) is completed within the same jurisdiction (that is, the originating VASP, the beneficiary VASP and any relevant intermediary VASP are located in the Bailiwick).

Application of other provisions of this Schedule.

15G. For the avoidance of doubt, the provisions of this Part of this Schedule –

(a) are in addition to and not in derogation from the application of the other provisions of this Schedule in respect of virtual assets (and transfers thereof) and VASPs, and

(b) apply to any specified business when acting in respect of a virtual asset transfer on behalf of a customer as they apply to originating VASPs, beneficiary VASPs or intermediary VASPs, as the case may be.]

[PART IIIB

PROVISIONS APPLICABLE TO TRUSTEES AND PARTNERS

Application.

15H. This Part applies to any specified business that –

(a) carries out regulated activities within the meaning of Schedule 1, and

[(b) in the course of those activities, acts as a trustee of a relevant trust or a partner of a relevant partnership (or occupies an equivalent role to that of trustee or partner in relation to a foreign legal arrangement).]

Regulated agents and service providers.

15I. (1) [Where a specified business to which this Part applies is acting as a trustee of a relevant trust or a partner of a relevant partnership, it] must hold information on the identity of any regulated agents and service providers to the relevant trust or relevant partnership, as the case may be.

(2) A specified business that holds information within subparagraph (1) must ensure that the information –

(a) so far as is possible, is accurate and up to date, and

(b) is updated on a timely basis.

Disclosure of status.

15J. (1) Where –

(a) a specified business to whom this Part applies –

(i) enters into a business relationship with, or

(ii) carries out or is otherwise involved in an occasional transaction with,

a financial services business or a relevant business, and

(b) the specified business is carrying out the activity at subparagraph (a) in its capacity as a trustee of a relevant trust or a partner of a relevant partnership [(or the occupant of an equivalent role in relation to a foreign legal arrangement)], as the case may be,

the specified business must disclose the matters in subparagraph (b) to the financial services business or relevant business in question.

(2) The provisions of this paragraph are without prejudice to any powers or duties of disclosure that may otherwise be applicable.

Disclosure of information.

15K. (1) A specified business within paragraph 15H may disclose upon request –

(a) to any of the relevant authorities, any information relating to the trust or partnership, as the case may be, and

(b) in the circumstances described in paragraph 15J(1)(a), to a financial services business or relevant business, any information relating to –

(i) the beneficial ownership of the trust or partnership, as the case may be, and

(ii) any assets of the trust or partnership, as the case may be, that are to be held or managed under the terms of a business relationship or occasional transaction in question.

(2) The provisions of this paragraph are without prejudice to any powers or duties of disclosure that may otherwise be applicable.]

PART IV

DESIGNATION OF SUPERVISORY AUTHORITY

Guernsey Financial Services Commission.

16. (1) The Commission is prescribed as the supervisory authority with responsibility for monitoring and enforcing compliance by specified businesses with paragraphs and other measures made or issued under this Law, or any other enactment, for the purpose of forestalling, preventing or detecting money laundering and terrorist financing.

(2) When exercising its functions under subparagraph (1), the Commission must take into account information on, or in relation to, the money laundering and terrorist financing risk associated with particular countries, territories and geographic areas and the level of cooperation it expects to receive from relevant authorities in those countries, territories and areas, including information contained in the Financial Action Task Force Recommendations, and the NRA.

[(2A) For the avoidance of doubt, and without prejudice to the functions of the Commission under any other enactment or any action taken by the Commission under such an enactment, the functions of the Commission in subparagraph (1) include monitoring and enforcing compliance by specified businesses with any international sanctions measure that has been implemented in the Bailiwick, and references to those functions shall be construed accordingly.]

(3) The Commission is also designated as the competent authority –

(a) to register financial service businesses under Schedule 4,

(b) ...

(c) to register prescribed businesses under Schedule 5.

(4) For the purpose of subparagraph (1), **"measures"** includes rules, guidance, instructions, notices and other similar instruments.

[**Proliferation financing etc.**

16A. (1) Subject to subparagraphs (3) and (4), and without prejudice to paragraph 6(2A), the provisions of this Schedule apply to the activity within subparagraph (2) in the same way that they apply to money laundering and terrorist Financing, and shall he construed accordingly.

(2) The activity within this subparagraph is the breach of targeted financial sanctions that –

(a) are imposed under any international sanctions measure that has been implemented in the Bailiwick, and

(b) relate to the proliferation of weapons of mass destruction and its financing,

and for the avoidance of doubt, the breach of targeted financial sanctions includes their non-implementation. circumvention or evasion.

(3) Subparagraph (1) does not apply to –

(a) paragraph 10(2)(b)(ii), or

(b) subparagraph (B) in the definition of Appendix C business in paragraph 21.

(4) For the purposes of subparagraph (1), references in paragraph 3(8) to 31st March 2019 shall be read as references to 29th February, 2024.

(5) The references to the NRA in this Schedule include any national risk assessment in respect of the proliferation of weapons of mass destruction and its financing that may be published by the Committee as amended from time to time, and shall be construed

accordingly.]

PART V
MISCELLANEOUS

Notification etc: financial services businesses.

17. Any person who is a financial services business by virtue of providing money or value transmission services [within the meaning of [paragraph 4 or 6] of Part I of Schedule 1 or by virtue of falling within paragraph 27(2) of Part I of Schedule 1 (VASPs)] shall maintain a current list of its agents for such services, [which shall be made available on demand to –

(a) the Commission, and

(b) any supervisory authority that exercises, in a jurisdiction outside the Bailiwick where the financial services business or any of its agents operate, functions corresponding to any of the functions of the Commission under sections 2 and 3 of the Financial Services Commission (Bailiwick of Guernsey) Law, 1987].

Extension of sections 49B and 49C: prescribed businesses.

18. Sections 49B and 49C extend in respect of any prescribed business as if references in those sections to "financial services business" or "section 49" were references to "prescribed business" and "section 49A" respectively.

Offences as to false and misleading information.

19. If a person –

(a) in purported compliance with a requirement imposed by this Schedule, or

(b) otherwise than as mentioned in subparagraph (a) but in circumstances in which that person intends, or could reasonably be expected to know, that any statement, information or document provided by the person would or might be used by the

Commission for the purpose of exercising its functions conferred by this Schedule,

does any of the following –

(i) makes a statement which the person knows or has reasonable cause to believe to be false, deceptive or misleading in a material particular,

(ii) dishonestly or otherwise, recklessly makes a statement which is false, deceptive or misleading in a material particular,

(iii) produces or furnishes or causes or permits to be produced or furnished any information or document which the person knows or has reasonable cause to believe to be false, deceptive or misleading in a material particular, or

(iv) dishonestly or otherwise, recklessly produces or furnishes or recklessly causes or permits to be produced or furnished any information or document which is false, deceptive or misleading in a material particular,

the person is guilty of an offence and liable on conviction on indictment, to imprisonment not exceeding a term of five years or a fine or both or on summary conviction, to imprisonment for a term not exceeding 6 months or a fine not exceeding level 5 on the uniform scale or both.

Offences: general.

20. (1) Any person who contravenes any requirement of this Schedule shall be guilty of an offence and liable –

(a) on conviction on indictment, to imprisonment not exceeding a term of five years or a fine or both,

(b) on summary conviction, to imprisonment for a term not exceeding 6 months or a fine not exceeding level 5 on the Uniform Scale or both.

(2) In determining whether a person has contravened a requirement of this Schedule, a court may take account of –

(a) any rules and guidance in the Handbook, and

(b) any notice or instruction issued by the Commission under this Law,

that the court considers relevant to the requirement concerned.

(3) It is a defence for a person charged with an offence under this paragraph to prove that he or she has taken all reasonable precautions to avoid the commission of the offence.

Interpretation.

21. (1) In this Schedule, unless the context otherwise requires, expressions defined in this Law have those meanings, and –

"account" means a bank account and any other business relationship between a specified business and a customer which is of a similar nature having regard to the services offered by the specified business,

"Appendix C business" means –

(a) a financial services business supervised by the Commission, or

(b) a business which is carried on from –

(i) a country or territory listed in Appendix C to the Handbook and which would, if it were carried on in the Bailiwick, be a financial services business, or

(ii) the United Kingdom, the Bailiwick of Jersey, the Bailiwick of Guernsey or the Isle of Man by a lawyer or an accountant,

and, in either case, is a business –

(A) which may only be carried on in that country or territory by a person regulated for that purpose under the law of that country or territory,

(B) the conduct of which is subject to requirements to forestall, prevent and detect money laundering and terrorist financing that are consistent with those in the Financial Action Task Force Recommendations in respect of such a business, and

(C) the conduct of which is supervised for compliance with the requirements referred to in subparagraph (B), by the Commission or [a relevant supervisory authority],

[but does not include a business of the type described in paragraph 6 of Schedule 2,]

"bank" means a person who accepts deposits, including a person who does so in a country or territory outside the Bailiwick, in the course of carrying on a deposit-taking business within the meaning of the Banking Supervision (Bailiwick of Guernsey)

Law, 1994[zg] and related expressions shall be construed accordingly,

"bearer share" means a negotiable instrument that accords ownership in a legal person to the individual who possesses the relevant bearer share certificate,

"bearer warrant" means a warrant or other instrument entitling the holder to subscribe for shares or other investments in the capital of a company, title of which can be transferred by delivery,

"beneficial owner": see [paragraph 22],

the **"board"** of a specified business: see subparagraph (2),

a **"branch office"** of a business means a place of business of that business that is physically separate from that business and that has no legal personality,

"business relationship" means a business, professional or commercial relationship between a specified business and a customer which is expected by the specified business, at the time when contact is established, to have an element of duration,

"business risk assessment": see paragraph 3(3),

"correspondent banking relationship" means a business relationship which involves the provision of banking services by one bank to another bank (**"the respondent bank"**),

"customer" means a person or legal arrangement who –

---

zg Order in Council No. XIII of 1994; as amended by Order in Council No. XVII of 2002; No. XXI of 2002; No. XVI of 2003; No. XVI of 2008; No. IV of 2009; No. XIII of 2010; No. XXI of 2010; Ordinance No. XXXIII of 2003; No. XII of 2015; No. XX of 2015; No. XXXIX of 2015; No. II of 2016; No. IX of 2016; No. XXVII of 2017; Alderney Ordinance No. III of 2017; Sark Ordinance No. X of 2017; G.S.I. No. 3 of 2000; G.S.I. No. 1 of 2008; G.S.I. No. 35 of 2010; G.S.I. No. 83 of 2010; and G.S.I. No. 50 of 2017.

(a) is seeking to establish, or has established, a business relationship with a specified business, or

(b) is seeking to carry out, or has carried out, an occasional transaction with a specified business,

except that where such a person or legal arrangement is an introducer, the customer is the person or legal arrangement on whose behalf the introducer is seeking to establish or has established the business relationship,

"customer due diligence" means the steps which a specified business is required to carry out pursuant to paragraph 4(3),

"customer due diligence information" means –

(a) identification data,

(b) any account files and correspondence relating to the business relationship or occasional transaction, and

(c) all records obtained through customer due diligence measures, including the results of any analysis undertaken,

"Disclosure Law" means the Disclosure (Bailiwick of Guernsey) Law, 2007[zh],

"Economic Crime Division" means that branch of the Customs and Immigration Service responsible for the investigation of financial and economic crime,

"employee" means an individual working, including on a temporary basis, for

---

zh Order in Council No. XVI of 2007; as amended by Ordinance No. XXXIX of 2008; No. VII of 2009; Nos. XIV, XIX and No. XXXVII of 2010; Nos. XVI and LIII of 2014; No. XXXIX of 2015; and No. IX of 2016.

a specified business whether under a contract of employment, a contract for services or otherwise,

"enhanced customer due diligence": see paragraph 5(3)(a),

"enhanced measures": see paragraph 5(3)(b),

"Financial Action Task Force Recommendations" means the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation issued by the Financial Action Task Force as revised or reissued from time to time,

[**"Financial Intelligence Unit"** has the meaning given in Part III of the Economic and Financial Crime Bureau and Financial Intelligence Unit (Bailiwick of Guernsey) Law, 2022,]

"foundation" means –

(a) a foundation created under the Foundations (Guernsey) Law, 2012[zi], or

(b) an equivalent or similar body created or established under the law of another jurisdiction (and howsoever named),

"foundation official" means –

(a) in relation to a foundation created under the Foundations (Guernsey) Law, 2012, a foundation official within the meaning of that Law, and

---

zi Order in Council No. I of 2013; as amended by Order in Council No. VI of 2017; and Ordinance No. IX of 2016.

(b) in relation to an equivalent or similar body created or established under the law of another jurisdiction, a person with functions corresponding to those of a foundation official described in paragraph (a),

"founder" means –

(a) in relation to a foundation created under the Foundations (Guernsey) Law, 2012, a founder within the meaning of that Law, and

(b) in relation to an equivalent or similar body created or established under the law of another jurisdiction, a person corresponding to a founder described in paragraph (a),

"the FSB Regulations" means the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2007,

"funds" means assets of all types, [including, for the avoidance of doubt, virtual assets,] and documents or instruments evidencing title to or an interest in such assets,

"Handbook" means the Handbook on Countering Financial Crime and Terrorist Financing, as revised or re-issued from time to time by the Commission,

"high risk relationship" means a business relationship or an occasional transaction which has a high risk of involving money laundering or terrorist financing and related terms shall be construed accordingly,

"identification data" means documents, data and information from a reliable and independent source,

"international organisation" means an entity –

(a) which was established by a formal political agreement between its member states that has the status of an international treaty,

(b) the existence of which is recognised by law in its member states, and

(c) which is not treated as a resident institutional unit of the country in which it is located,

"introducer" means an Appendix C business who is seeking to establish or has established, on behalf of another person or legal arrangement who is its customer, a business relationship or an occasional transaction with a specified business,

"joint arrangement" has the same meaning as in regulation 5 of the Beneficial Ownership (Definition) Regulations, 2017,

"joint interests" has the same meaning as in regulation 4 of the Beneficial Ownership (Definition) Regulations, 2017,

"legal arrangement" includes an express trust and any vehicle or arrangement whatsoever which has a similar legal effect to an express trust,

"low risk relationship" means a business relationship or an occasional transaction which has a low risk of involving money laundering or terrorist financing and related terms shall be construed accordingly,

"minimum retention period" means –

(a) in the case of any customer due diligence information –

(i) a period of five years starting from the date –

(A) where the customer has established a business relationship with the specified business, that relationship ceased,

(B) where the customer has carried out an occasional transaction with the specified business, that transaction was completed, or

(ii) such other longer period as the Commission may direct,

(b) in the case of a transaction document –

(i) a period of five years starting from the date that both the transaction and any related transaction were completed, or

(ii) such other longer period as the Commission may direct,

[**"Money Laundering Compliance Officer"** means a person of at least manager level appointed by a specified business to monitor compliance with policies, procedures and controls to forestall, prevent and detect money laundering and terrorist financing,]

[**"Money Laundering Reporting Officer"** means a person of at least manager level appointed by a specified business to make or receive disclosures under Part I of the Disclosure Law and sections 12, 15 and 15A of the Terrorism Law,]

"nominee shareholder" has the same meaning as "nominee" has in the Beneficial Ownership of Legal Persons (Nominee Relationships) Regulations, 2017[zj],

"notify" means notify in writing,

[zj] G.S.I. No. 102 of 2017; as amended by G.S.I. No. 120 of 2017.

"NRA" means the National Risk Assessment published by the Committee as amended from time to time,

"occasional transaction" means any transaction involving more than £10,000 [(or [£1,000 or more] in the case of a specified business described in paragraph 27(2) of Schedule 1 ("VASPs"))], carried out by the specified business in question in the course of that business, where no business relationship has been proposed or established and includes such transactions carried out in a single operation or two or more operations that appear to be linked,

"the PB Regulations" means Criminal Justice (Proceeds of Crime) (Legal Professionals, Accountants and Estate Agents) (Bailiwick of Guernsey) Regulations, 2008,

"politically exposed person": see paragraph 5(4),

"prescribed business" means any business which is a relevant business for the purposes of this Law, but does not include a business of a type described in paragraphs 2 or 4 of Schedule 2,

"protector" has the meaning in section 58 of the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc. (Bailiwick of Guernsey) Law, 2000[zk],

[**"regulated agent"** means a person who –

(a) is acting in relation to or on behalf of a relevant trust or relevant partnership, as the case may be, and

---

zk Order in Council No. I of 2001; as amended by No. I of 2000; No. VIII of 2008; No. XXV of 2008; No. XIII of 2010); No. XIX of 2010; No. I of 2013; Ordinance No. XXXVII of 2001; No. XXXIII of 2003; No. VII of 2009; No. XII of 2015; No. XXXIX of 2015; No. II of 2016; No. IX of 2016; No. XXVII of 2017; Alderney Ordinance No. III of 2017; Sark Ordinance No. X of 2017; G.S.I. No. 3 of 2008; G.S.I. No. 83 of 2010; G.S.I. No. 4 of 2013; G.S.I. No. 50 of 2017; G.S.I. No. 56 of 2017; and G.S.I. No. 72 of 2017.

(b) for the purposes of so doing is required to hold, and does hold, a licence from the Commission or a corresponding body in another jurisdiction,]

[**"relevant authorities"** means –

(a) His Majesty's Procureur,

(b) a police officer,

(c) the Committee,

(d) the Commission,

(e) the Alderney Gambling Control Commission,

(f) the Director of the Economic and Financial Crime Bureau,

(g) the Financial Intelligence Unit,

(h) the Director of the Revenue Service,

(i) the Registrar of Charities and other Non Profit Organisations,

(j) the Registrar of Non-Profit Organisations appointed under the Charities and Non-Profit Organisations (Registration) (Sark) Law, 2010,

(k) the Registrar for the purposes of each of the Beneficial Ownership Laws,

(l) the Registrar of Companies,

(m) the Registrar of Limited Liability Partnerships,

(n) the Registrar of Foundations,

(o) the Greffier, and

(p) the Registrar for the purposes of the Companies (Alderney) Law, 1994,]

"**relevant employee**" means any –

(a) member of the board of the specified business,

(b) member of the management of the specified business, and

(c) employee whose duties relate to the specified business,

the "**relevant enactments**" means –

(a) this Law,

(b) the Drug Trafficking (Bailiwick of Guernsey) Law, 2000[zl],

(c) the Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011[zm],

[(d) the Sanctions (Bailiwick of Guernsey) Law, 2018,]

---

zl Order in Council No. VII of 2000; amended by Order in Council No. I of 2000; No. II of 2005; Nos. XVI and XVII of 2007; No. XIII of 2010; Ordinance No. XXXIII of 2003; No. XXXVIII of 2008; Nos. XV and XXV of 2010; No. XVI of 2014; and No. IX of 2016.

zm Order in Council No. XI of 2011; amended by Ordinance No. IX of 2016.

[(e) any UK enactment within the meaning of, and as implemented by, the Sanctions (Implementation of UK Regimes) (Bailiwick of Guernsey) (Brexit) Regulations, 2020,]

(f) ...

(g) ...

(h) ...

(i) ...

(j) the Terrorism Law,

(k) the Disclosure Law,

(l) the Transfer of Funds (Guernsey) Ordinance, 2017[zt],

(m) the Transfer of Funds (Alderney) Ordinance, 2017[zu],

(n) the Transfer of Funds (Sark) Ordinance, 2017[zv],

(o) the Disclosure (Bailiwick of Guernsey) Regulations, 2007[zw],

(p) the Terrorism and Crime (Bailiwick of Guernsey) Regulations, 2007[zx],

---

zt Ordinance No. XXVII of 2017.

zu Alderney Ordinance No. III of 2017.

zv Sark Ordinance No. X of 2017.

zw G.S.I. No. 34 of 2007.

zx G.S.I. No. 36 of 2007; as amended by G.S.I. No. 27 of 2008; G.S.I. No. 49 of 2010; G.S.I. No. 24 of 2011; and G.S.I. No. 51 of 2014.

(q) ...

(r) the Prescribed Businesses (Bailiwick of Guernsey) Law, 2008[zy],

(s) the Beneficial Ownership of Legal Persons (Guernsey) Law, 2017[zz],

(t) the Beneficial Ownership of Legal Persons (Alderney) Law, 2017[zaa],

(u) the Beneficial Ownership (Definition) Regulations, 2017,

(v) the Beneficial Ownership (Alderney) (Definition) Regulations, 2017[zbb],

(w) the Beneficial Ownership of Legal Persons (Provision of Information) (Transitional Provisions) Regulations, 2017[zcc],

(x) the Beneficial Ownership of Legal Persons (Provision of Information) (Transitional Provisions) (Alderney) Regulations, 2017,

(y) the Beneficial Ownership of Legal Persons (Nominee Relationships) Regulations, 2017,

---

zy Order in Council No. XII of 2009; as amended by Ordinance No. XXXIX of 2015; Nos. II and IX of 2016; Alderney Ordinance No. III of 2017; Ordinance No. XXVII of 2017; and Sark Ordinance No. X of 2017.

zz Order in Council No. VI of 2017; as amended by Ordinance No. XXVIII of 2017.

zaa Order in Council No. VII of 2017; as amended by Alderney Ordinance No. X of 2017.

zbb Alderney Statutory Instrument No. 3 of 2017.

zcc G.S.I. No. 87 of 2017.

(z) the Beneficial Ownership of Legal Persons (Nominee Relationships) (Alderney) Ordinance, 2017[zdd],

(aa) the Beneficial Ownership of Legal Persons (Provision of Information) (Limited Partnerships) Regulations, 2017[zee],

and such other enactments relating to money laundering and terrorist financing as may be enacted from time to time in the Bailiwick,

"relevant legal person" has the meaning given in the Beneficial Ownership of Legal Persons (Guernsey) Law, 2017,

[**"relevant supervisory authority"** has the meaning given in section 59(1) of the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc (Bailiwick of Guernsey) Law, 2020,]

"risk" means a risk of money laundering or terrorist financing occurring and "risk assessment" shall be construed accordingly,

[**"service provider"** means a person, other than a regulated agent, who is providing investment advisory or management services, managerial services, accountancy services, tax advisory services, legal services, trust services, partnership services or corporate services in relation to a relevant trust or relevant partnership, as the case may be,]

"specified business": see paragraph 1(1),

"subordinate legislation" means any ordinance, statutory instrument, paragraph, rule, order, notice, rule of court, resolution, scheme, warrant, byelaw or other

---

zdd Alderney Ordinance No. XI of 2017.

zee G.S.I. No. 120 of 2017.

instrument made under any enactment and having legislative effect,

"Terrorism Law" means the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002[zff],

"terrorist financing" has the meaning given in the Terrorism Law,

"transaction document": see paragraph 14, [...]

[**"VASPs"** and **"virtual asset"**: see paragraph 15B,]

"voting rights" has the same meaning as in regulation 7 of the Beneficial Ownership (Definition) Regulations, 2017.

(2) Subject to subparagraph (3), in this Ordinance the **"board"** of a specified business means –

(a) the board of directors of that specified business, where it is a body corporate, or

(b) the senior management of a specified business, where it is not a body corporate.

(3) References in this Ordinance to the board of a specified business shall, where the specified business is a sole trader, be construed consistently with the provisions of the Handbook.

(4) References in this Schedule to **"forming a suspicion"** of money laundering or terrorist financing, and any related expressions, are references to a person –

---

zff Order in Council No. XVI of 2002; as amended by Order in Council No. I of 2000; No. VII of 2005; No. XIII of 2006; No. XIII of 2010; No. XI of 2011; No. XIV of 2012; Ordinance No. XXXIII of 2003, No. XLVI of 2007; No. XIII of 2010; No. XX of 2010; No. XXXVII of 2010; No. XXIX of 2014; No. LIV of 2014; No. IX of 2016; G.S.I. No. 16 of 2003; G.S.I. No. 41 of 2005; and G.S.I. No. 5 of 2017.

(a) knowing or suspecting, or

(b) having reasonable grounds for knowing or suspecting,

that another person is engaged in –

(i) money laundering or that certain property is or is derived from the proceeds of criminal conduct (within the meaning of the Disclosure Law), or

(ii) terrorist financing or that certain property is or is derived from terrorist property (within the meaning of the Terrorism Law),

as the case may be.

Meaning of "beneficial owner".

22. (1) References in this Schedule to a **"beneficial owner"** are to be construed in accordance with subparagraphs (2) to (11).

(2) In relation to a legal person, **"beneficial owner"** means, subject to subparagraphs (3) to (11) –

(a) the natural person who ultimately controls the legal person through ownership; or if no such person exists or can be identified,

(b) the natural person who ultimately controls the legal person through other means; or, if no such person exists or can be identified,

(c) the natural person who holds the position of a senior managing official of the legal person.

(3) In any case where –

(a) the natural person who controls the legal person through ownership has been identified,

(b) there are reasonable grounds to believe that the legal person is also ultimately controlled by another natural person through other means, and

(c) that other natural person can be identified,

[both the persons described in (2)(a) and (b) are a beneficial owner in relation to the legal person].

(4) In any case where a trust or other legal arrangement controls a legal person through ownership, the beneficial owners of that legal person are the beneficial owners of that trust or legal arrangement as defined in subparagraphs (8) and (9).

(5) In any case where a transparent legal person has control of a legal person through ownership (**"the controlled legal person"**), that transparent legal person shall be treated as a natural person for the purposes of this Schedule, and therefore (for the avoidance of doubt) as the beneficial owner of the controlled legal person.

(6) For the purposes of subparagraph (2), a person has control of a legal person through ownership if that person holds, directly or indirectly, any of the following –

(a) if the legal person is a company –

(i) more than 25% of the shares in the company,

(ii) more than 25% of the voting rights in the company, or

(iii) the right to appoint or remove directors holding a majority of voting rights on all or substantially all matters at meetings of the board,

(b) if the legal person is any other form of legal person other than a foundation,

(i) more than 25% of the shares in the legal person or an interest equivalent to a shareholding of more than 25%, including but not limited to an entitlement to more than 25% of the assets of the legal person in the event of its winding up or dissolution,

(ii) more than 25% of the voting rights in the conduct or management of the legal person, or

(iii) the right to appoint or remove a majority of the managing officials of the legal person holding a majority of voting rights on all or substantially all matters at meetings of the legal person that are equivalent to board meetings.

(c) if the legal person is a foundation,

(i) any of the rights and interests under subparagraph (6)(b)(i) to (iii), or

(ii) a vested beneficial interest or future entitlement to benefit from more than 25% of the assets of the foundation,

and for the purposes of this paragraph, holding more than 25% of the shares in a company means holding a right or rights to share in more than 25% of the capital or, as the case may be, the profits of the company.

(7) A person holds shares or rights for the purposes of subparagraph (6) if –

(a) those shares or rights constitute joint interests,

(b) those shares or rights are held under a joint arrangement,

(c) those shares or rights are held on behalf of that person by a nominee,

(d) in the case of rights, that person controls their exercise,

(e) in the case of rights only exercisable in certain circumstances, those rights are to be taken into account,

(f) in the case of rights attached to shares held by way of security provided by a person, the rights are still exercisable by that person.

(8) In relation to a trust, [**"beneficial owner"** means, for the purposes of this Schedule –]

(a) any beneficiary who is a natural person, whether his or her interest under the trust is vested, contingent or discretionary, and whether that interest is held directly by that person or as the beneficial owner of a legal person or a legal arrangement that is a beneficiary of the trust,

(b) any trustee, settlor, protector or enforcer of the trust who is a natural person or that is a transparent legal person,

(c) if any trustee, settlor, protector or enforcer of the trust is a legal person (other than a transparent legal person), or a legal arrangement, any natural person who is the beneficial owner of that legal person or legal arrangement,

(d) any natural person (other than a beneficiary, trustee, settlor, protector or enforcer of the trust), who has, under the trust deed of the trust or any similar document, power to –

(i) appoint or remove any of the trust's trustees,

(ii) direct the distribution of funds or assets of the trust,

(iii) direct investment decisions of the trust,

(iv) amend the trust deed, or

(v) revoke the trust,

(e) any transparent legal person (other than a trustee, settlor, protector or enforcer of the trust) that has any of the powers set out in subparagraph (d),

(f) where a legal person (other than a transparent legal person) or a legal arrangement holds any of the powers within subparagraph (d) (other than a trustee, settlor, protector or enforcer of the trust), any natural person who is a beneficial owner of that legal person or legal arrangement, and

(g) any other natural person who exercises ultimate effective control over the trust.

(9) In relation to a legal arrangement other than a trust, **"beneficial owner"** means any natural person or transparent legal person who is in a position in relation to that legal arrangement that is equivalent to the position of any natural person or transparent legal person set out at subparagraph (8).

(10) For the purposes of this paragraph, **"transparent legal person"** means –

(a) a company that is listed on a recognised stock exchange within the meaning of the Beneficial Ownership (Definition) Regulations, 2017, or a majority owned subsidiary of such a company,

(b) a States trading company within the meaning of the States Trading Companies (Bailiwick of Guernsey) Law, 2001[zgg],

(c) a legal person controlled by the States of Alderney through ownership within the meaning of the Beneficial Ownership (Alderney) (Definition) Regulations, 2017 (or any successor regulations made under section 25 of the Beneficial Ownership of Legal Persons (Alderney) Law, 2017, or

(d) a regulated person within the meaning of section 41(2) of the Beneficial Ownership of Legal Persons (Guernsey) Law, 2017.

(11) For the purposes of this paragraph –

(a) a reference (however expressed) to a person controlling the exercise of a right is to be construed consistently with regulation 10(2) of the Beneficial Ownership (Definition) Regulations, 2017,

(b) a reference (however expressed) to taking rights into account is to be construed consistently with regulation 11 of the Beneficial Ownership (Definition) Regulations, 2017, and

---

zgg Order in Council No. XII of 2001.

(c) a reference (however expressed) to rights being exercisable by a person is to be construed consistently with regulation 12(a) and (b) of the Beneficial Ownership (Definition) Regulations, 2017.]

NOTES

Schedule 3 was inserted by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) Ordinance, 2018, section 1(12), Schedule 1, with effect from 31st March, 2019, subject to the transitional and saving provisions in section 3 of the 2018 Ordinance.

In Schedule 3,

first, the words, parentheses and figures in square brackets in paragraph 1(1) and, second, the words in square brackets in paragraph 1(2) were substituted, third, paragraph 1(3) was inserted, fourth, paragraph 6(1) and, fifth, paragraph 6(2)(b) were substituted, sixth, the words in square brackets in paragraph 7(2)(c) were substituted, seventh, paragraph 7(3) was inserted, eighth, the word in square brackets in paragraph 11(1)(b) was substituted, ninth, the words in square brackets in paragraph 12(4) were substituted and paragraph 12(5) was inserted, tenth, paragraph 13(2A) and the words in square brackets in paragraph 13(2) were both inserted, eleventh, paragraph 14(7) and, twelfth, the words in the second pair of square brackets in the definition of the expression "Appendix C business) were both inserted by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) (No. 2) Regulations, 2023, regulation 1, respectively paragraph (2)(a)(i), paragraph (2)(a)(ii), paragraph (2)(a)(iii), paragraph (2)(b)(i), paragraph (2)(b)(ii), paragraph (2)(c)(i), paragraph (2)(c)(ii), paragraph (2)(d), paragraph (2)(e), paragraph (2)(f), paragraph (2)(g) and paragraph (2)(h), with effect from 8th July, 2023 and, in accordance with the transitional provisions of regulation 2(1) of the (No. 2) Regulations, paragraph 20 of this Schedule shall not apply to a paragraph 2(3A) business (as defined in regulation 2(2) thereof) until 1st October 2023;

first, at the end of paragraph 3(3)(c)(ii) the punctuation in square brackets was substituted and the words in square brackets thereafter were inserted, second, paragraph 15(1)(ba) was inserted and, third, the word in square brackets in paragraph 15(2) was substituted by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) (No. 3) Regulations, 2023, respectively regulation 1(2), regulation 1(3) and regulation 1(4),with effect from 8th July, 2023;

first, the words in square brackets in paragraph 4(3)(c), second, paragraph 5(3)(a)(ii), third, the word, symbol and figures in paragraph 15(C)(1)(e), fourth, the word, symbol and figures in paragraph 15(C)(2)(c),
fifth, paragraph 15H(b) was substituted and sixth, the words in square brackets in paragraph 15I(1) were all substituted, seventh, the words in square brackets in paragraph 15J(1)(b) were inserted and, eighth, the symbol, figures and words in square brackets within the square brackets in the definition of the expression "occasional transaction" in paragraph 21(1) were substituted by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment of Schedule 3) (No. 3) Regulations, 2024, respectively regulation 1(2), regulation 1(3), regulation 1(4), regulation 1(5), regulation 1(6), regulation 1(7), regulation 1(8) and regulation 1(9), with effect from 22nd April, 2024;

first, paragraph 4(7), second, the words in square brackets in paragraph 5(4) and third, the words in square brackets in paragraph 5(4)(d) were substituted, fourth, paragraph 5A was inserted, fifth, the words in square brackets in paragraph 12(1)(a) and paragraph 15(1)(a), sixth, the word and figures in square brackets in the definition of the expression "beneficial owner" in paragraph 21, and the definitions of the expressions "Money Laundering Compliance Officer" and "Money Laundering Reporting Officer" in that paragraph, and, seventh, the words in square brackets in paragraph 22(8) were substituted by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) Regulations, 2019, respectively regulation 2, regulation 3(a), regulation 3(b), regulation 4, regulation 5, regulation 6 and regulation 7, with effect from 13th June, 2019;

first, the figures, parentheses, letters and word in square brackets in paragraph 9, second, the words and figure in paragraph 17 and, third, the words, parentheses and letters in square brackets in paragraph 22(3) were substituted by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment of Schedule 3) (No. 2) Regulations, 2024, respectively regulation 1(2), regulation 1(3) and regulation 1(4), with effect from 6th March, 2024;

first, the words in square brackets in paragraph 10(2)(b)(iii) were substituted, second, Part IIIA and paragraphs 15A to 15G thereof were inserted, third, paragraph 16(3)(b) was repealed, fourth, the words in square brackets in paragraph 17 were inserted, the words in square brackets in paragraph 21(1) in the definitions of the expressions, fifth, "Appendix C business" (the first pair of square brackets therein) were substituted, sixth, "funds" and, seventh, "occasional transaction" were both inserted, eighth, paragraph (q) of the definition of the expression "relevant enactments" in paragraph 21(1) was repealed, ninth, the definition of the expression "relevant supervisory authority" therein was inserted and, tenth, the word omitted in square brackets after the definition of the expression "transaction document" was repealed and the definition of the expressions "VASPs" and "virtual asset" in paragraph 21(1) was inserted by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) (No. 2) Ordinance, 2023, section 4, respectively paragraph (a), paragraph (b), paragraph (c), paragraph (d), paragraph (e)(i), paragraph (e)(ii), paragraph (e)(iii), paragraph (e)(iv), paragraph (e)(v) and paragraph (e)(vi), with effect from 7th July, 2023;

first, Part IIIB and paragraphs 15H to 15K thereof were inserted and, second, the definitions of the expressions "regulated agent", "relevant authorities" and "service provider" in paragraph 21(1) were inserted by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Trustees and Partners) (Amendment) Regulations, 2023, respectively regulation 1(4) and regulation 1(5), with effect from 8th July, 2023;

the words "Financial Intelligence Unit" in square brackets, wherever occurring, were substituted by the Criminal Justice (Miscellaneous Amendments) (Bailiwick of Guernsey) Ordinance, 2022, section 11, with effect from 21st December, 2022;

first, paragraph 16(2A) and, second, paragraph 16A were inserted, third, subparagraph (d) and, fourth, subparagraph (e) of the definition of the expression "relevant enactments" were substituted and, fifth, subparagraphs (f) to (i) of that definition were repealed by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment of Schedule 3) Regulations, 2024, respectively regulation 1(2), regulation 1(3), regulation 1(4)(a), regulation 1(4)(b) and regulation 1(4)(c), with effect from 6th February, 2024;

the words in the second pair of square brackets in paragraph 17 were substituted by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment of Schedule 3) (No. 4) Regulations, 2024, regulation 1, with effect from 24th April. 2024;

the definition of the expression "Financial Intelligence Unit" in paragraph 21 was substituted by the Economic and Financial Crime Bureau and Financial Intelligence Unit (Bailiwick of Guernsey) Law, 2022, section 11(1) and section 11(3)(c), with effect from 20th October, 2022.

The following Handbooks containing the rules and guidance referred to in paragraph 3(7) of this Schedule have been issued by the Guernsey Financial Services Commission:

Handbook on Countering Financial Crime and Terrorist Financing, 2019 (March, G.S.I. No. 75 of 2019);

Handbook on Countering Financial Crime and Terrorist Financing, 2019 (June, G.S.I. No. 76 of 2019);

Handbook on Countering Financial Crime and Terrorist Financing (G.S.I. No. 146 of 2023);

Handbook on Countering Financial Crime (AML/CFT/CPF) (G.S.I. No. 43 of 2024).

The Banking Supervision (Bailiwick of Guernsey) Law, 1994 and the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc (Bailiwick of Guernsey) Law, 2000 have both since been repealed by, respectively, the Banking Supervision (Bailiwick of Guernsey) Law, 2020, section 67(a), with effect from 1st November, 2021, subject to the savings and transitional provisions in section 68 of the 2020 Law; and the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc (Bailiwick of Guernsey) Law, 2020, section 62(a), with effect from 1st November, 2021, subject to the savings and transitional provisions in section 60 of the 2020 Law.

The Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2007 and the Criminal Justice (Proceeds of Crime) (Legal Professionals, Accountants and Estate Agents) (Bailiwick of Guernsey) Regulations, 2008 have both since been revoked by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) Ordinance, 2018, section 2, with effect from 31st March, 2019, subject to the transitional and saving provisions in section 3 of the 2018 Ordinance.

The Beneficial Ownership of Legal Persons (Provision of Information) (Limited Partnerships) Regulations, 2017 have since been revoked by the Limited Partnerships Guernsey) Law, 1995 (Amendment) Regulations, 2023, regulation 3(1), with effect from 13th September, 2023, subject to the provisions of regulation 3(2) of the 2023 Regulations.

Appendix H

High Risk Jurisdictions Subject to a Call for Action by the FATF

In accordance with Paragraph 5(1)(c)(i) of *Schedule 3*, the firm shall apply *ECDD* measures to a *business relationship* or *occasional transaction* where the *customer* or *beneficial owner* has a *relevant connection* with a country or territory that -

(A) provides funding or support for terrorist activities, or does not apply (or insufficiently applies) *the FATF Recommendations*, or
(B) is a country otherwise identified by the FATF as a country for which such measures are appropriate.

For the purposes of applying Paragraph 5(1)(c)(i) of *Schedule 3*, Appendix H to this *Handbook* identifies those countries and territories which the FATF has listed as high *risk*.

Democratic People's Republic of Korea	FATF Statement of 21 February 2020
Iran	FATF Statement of 21 February 2020
Myanmar (Burma)	FATF Statement of 21 October 2022

Appendix I

Countries and territories that are identified by relevant external sources as presenting a higher risk of ML, TF and/or PF

Appendix I lists countries and territories that are identified by the UK, US governments, intergovernmental and supranational organisations as presenting certain *ML, TF* and/or *PF* risks. Alongside these sources, information is presented reflecting assessments of a country or territory by non-governmental organisations and think tanks which firms may also find useful when they are determining the level of country *risk* presented by a *business relationship* or *occasional transaction. The Commission* does not accept responsibility for the findings and conclusions of these sources. The inclusion of a country or territory in Appendix I does not automatically imply that a *business relationship* or *occasional transaction* with a *relevant connection* to a country or territory on Appendix I is high *risk*, as the firm can continue to take a *risk* based decision on the level of overall *risk* within a *business relationship* or *occasional transaction* as set out in Section 3.4 of this *Handbook*. Please note that those countries and territories in relation to which the FATF has called for the application of countermeasures and therefore the firm must apply *ECDD* measures to a *business relationship* or *occasional transaction* where the *customer* or *beneficial owner* has a *relevant connection* with one of those countries or territories are listed in Appendix H.

	Intergovernmental and Supranational Organisations, UK and US Government Sources							**Non-Governmental Organisations and Think Tanks**			
Country/territory	**FATF – jurisdictions under increased monitoring**	**OECD – jurisdictions that have yet to implement agreed tax standards**	**INCSR (US Department of State) – Major drug producing and transit countries**	**Worldwide Governance Indicators project (World Bank)**	**Human Trafficking – US Department of State**	**State sponsors of terrorism - US Treasury Country Reports on Terrorism – US Department of State**	**UK HM Treasury Sanctions**	**TRACE Bribery Risk Matrix 2023**	**Transparency International – Corruptions Perception Index 2023**	**Fund for Peace/ Foreign Policy magazine – Fragile States Index (Alert level)**	**Global Terrorism Index 2024**
	Source:1	*Source:2*	*Source:3*	*Source:4*	*Source:5*	*Source:6*	*Source:7*	*Source:8*	*Source:9*	*Source:10*	*Source:11*
Afghanistan			✓	✓	✓	✓	✓	✓	✓	✓	✓
Algeria	✓			✓							
Angola	✓			✓						✓	
Argentina			✓								
Azerbaijan				✓					✓		

Country/territory	FATF – jurisdictions under increased monitoring	OECD – jurisdictions that have yet to implement agreed tax standards	INCSR (US Department of State) – Major drug producing and transit countries	Worldwide Governance Indicators project (World Bank)	Human Trafficking – US Department of State	State sponsors of terrorism - US Treasury Country Reports on Terrorism – US Department of State	UK HM Treasury Sanctions	TRACE Bribery Risk Matrix 2023	Transparency International – Corruptions Perception Index 2023	Fund for Peace/ Foreign Policy magazine – Fragile States Index (Alert level)	Global Terrorism Index 2024
Bangladesh				✓					✓	✓	
Belarus				✓	✓		✓				
Belize			✓								
Benin				✓							
Bolivia	✓			✓					✓		
Bosnia and Herzegovina				✓			✓				
British Virgin Islands	✓										
Bulgaria	✓										
Burkina Faso				✓						✓	✓
Burundi				✓					✓	✓	
Cambodia				✓	✓			✓	✓		
Cameroon	✓			✓					✓	✓	✓
Central African Republic				✓			✓	✓	✓	✓	
Chad				✓	✓			✓	✓	✓	
China				✓	✓						
Colombia						✓					✓
Comoros				✓				✓	✓		
Congo, Democratic Republic of	✓			✓			✓	✓	✓	✓	✓

Country/territory	FATF – jurisdictions under increased monitoring	OECD – jurisdictions that have yet to implement agreed tax standards	INCSR (US Department of State) – Major drug producing and transit countries	Worldwide Governance Indicators project (World Bank)	Human Trafficking – US Department of State	State sponsors of terrorism - US Treasury Country Reports on Terrorism – US Department of State	UK HM Treasury Sanctions	TRACE Bribery Risk Matrix 2023	Transparency International – Corruptions Perception Index 2023	Fund for Peace/ Foreign Policy magazine – Fragile States Index (Alert level)	Global Terrorism Index 2024
Congo Republic				✓				✓	✓	✓	
Costa Rica			✓								
Cote d'Ivoire (Ivory Coast)	✓			✓						✓	
Cuba				✓	✓	✓		✓			
Curaçao					✓						
Djibouti				✓	✓				✓		
Dominican Republic			✓								
Ecuador			✓	✓							
Egypt				✓							✓
El Salvador			✓	✓							
Equatorial Guinea				✓	✓			✓	✓		
Eritrea				✓	✓			✓	✓	✓	
Eswatini (Swaziland)				✓					✓		
Ethiopia				✓						✓	
Gabon				✓				✓	✓		
Gambia				✓							
Guatemala			✓	✓					✓		
Guinea				✓			✓		✓	✓	
Guinea Bissau			✓	✓	✓		✓		✓	✓	

Country/territory	FATF – jurisdictions under increased monitoring	OECD – jurisdictions that have yet to implement agreed tax standards	INCSR (US Department of State) – Major drug producing and transit countries	Worldwide Governance Indicators project (World Bank)	Human Trafficking – US Department of State	State sponsors of terrorism - US Treasury Country Reports on Terrorism – US Department of State	UK HM Treasury Sanctions	TRACE Bribery Risk Matrix 2023	Transparency International – Corruptions Perception Index 2023	Fund for Peace/ Foreign Policy magazine – Fragile States Index (Alert level)	Global Terrorism Index 2024
Guyana			✓								
Haiti	✓		✓	✓	✓		✓	✓	✓	✓	
Honduras			✓	✓					✓		
India											✓
Iraq				✓		✓	✓		✓	✓	✓
Jamaica			✓								
Kazakhstan				✓							
Kenya	✓		✓	✓						✓	
Kuwait	✓										
Kyrgyz Republic (Kyrgyzstan)				✓					✓		
Lao PDR[1]	✓			✓					✓		
Lebanon	✓			✓		✓	✓		✓	✓	
Lesotho				✓							
Liberia				✓					✓	✓	
Libya				✓	✓	✓	✓	✓	✓	✓	
Macau					✓						
Madagascar				✓					✓		
Malawi				✓							

[1] Lao PDR called Laos in earlier years.

Country/territory	FATF – jurisdictions under increased monitoring	OECD – jurisdictions that have yet to implement agreed tax standards	INCSR (US Department of State) – Major drug producing and transit countries	Worldwide Governance Indicators project (World Bank)	Human Trafficking – US Department of State	State sponsors of terrorism - US Treasury Country Reports on Terrorism – US Department of State	UK HM Treasury Sanctions	TRACE Bribery Risk Matrix 2023	Transparency International – Corruptions Perception Index 2023	Fund for Peace/ Foreign Policy magazine – Fragile States Index (Alert level)	Global Terrorism Index 2024
Mali				✓		✓	✓		✓	✓	✓
Mauritania				✓				✓	✓	✓	
Mexico			✓	✓							
Monaco	✓										
Mozambique				✓		✓			✓	✓	✓
Namibia	✓										
Nepal	✓			✓							
Nicaragua				✓	✓		✓	✓	✓		
Niger				✓						✓	✓
Nigeria			✓	✓					✓	✓	✓
Pakistan			✓	✓		✓			✓	✓	✓
Panama			✓								
Papua New Guinea	✓			✓	✓				✓		
Paraguay			✓	✓					✓		
Peru			✓	✓							
Philippines			✓	✓							
Russia				✓	✓		✓		✓		

Country/territory	FATF – jurisdictions under increased monitoring	OECD – jurisdictions that have yet to implement agreed tax standards	INCSR (US Department of State) – Major drug producing and transit countries	Worldwide Governance Indicators project (World Bank)	Human Trafficking – US Department of State	State sponsors of terrorism - US Treasury Country Reports on Terrorism – US Department of State	UK HM Treasury Sanctions	TRACE Bribery Risk Matrix 2023	Transparency International – Corruptions Perception Index 2023	Fund for Peace/ Foreign Policy magazine – Fragile States Index (Alert level)	Global Terrorism Index 2024
Sierra Leone				✓							
Sint Maartin					✓						
Somalia				✓	✓	✓	✓	✓	✓	✓	✓
South Sudan	✓			✓	✓		✓	✓	✓	✓	
Sri Lanka				✓						✓	
Sudan				✓		✓	✓		✓	✓	
Syria	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Tajikistan				✓					✓		
Tanzania				✓							
Timor-Leste (East Timor)				✓							
Togo				✓							
Trinidad & Tobago		✓									
Turkey				✓							
Turkmenistan				✓	✓			✓	✓		
Uganda				✓					✓	✓	
Ukraine				✓						✓	
Uzbekistan				✓							
Venezuela	✓		✓	✓	✓	✓	✓	✓	✓	✓	
Vietnam	✓			✓							
Yemen	✓			✓	✓	✓	✓	✓	✓	✓	
Zambia				✓							
Zimbabwe				✓			✓		✓	✓	
North Sinai						✓					

Country/territory	FATF – jurisdictions under increased monitoring	OECD – jurisdictions that have yet to implement agreed tax standards	INCSR (US Department of State) – Major drug producing and transit countries	Worldwide Governance Indicators project (World Bank)	Human Trafficking – US Department of State	State sponsors of terrorism - US Treasury Country Reports on Terrorism – US Department of State	UK HM Treasury Sanctions	TRACE Bribery Risk Matrix 2023	Transparency International – Corruptions Perception Index 2023	Fund for Peace/ Foreign Policy magazine – Fragile States Index (Alert level)	Global Terrorism Index 2024
The Lake Chad Region						✓					
The Trans-Sahara						✓					
The Southern Philippines						✓					
The Sulu/ Sulawesi Seas Littoral						✓					
West Bank and Gaza				✓						✓	

Relevant External Sources

1 Financial Action Task Force: Jurisdictions under Increased Monitoring (4 March 2026) - https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/outcomes-FATF-plenary-february-2026.html

2 OECD: Global Forum on Transparency and Exchange of Information for Tax Purposes – Peer Review of the Automatic Exchange of Financial Account Information (2023) – jurisdictions that have not yet exchanged information because their legal implementation is ongoing - https://www.oecd.org/en/publications/peer-review-of-the-automatic-exchange-of-financial-account-information-2023-update_5c9f58ae-en.html

3 United States Department of State: International Narcotics Strategy Report of March 2023 – countries where proceeds from drug trafficking significantly affects the U.S.A. - 2023-INCSR-Vol-2-Money-Laundering.pdf

4 Worldwide Governance Indicators project (2023 Update) – countries scoring an overall average of 40 per cent or less across the areas assessed for that country (voice and accountability, political stability (no violence), government effectiveness, regulatory quality, rule of law, and control of corruption) - http://info.worldbank.org/governance/wgi/#home

5 United States Department of State: Trafficking in Persons Report (June 2024) – Tier 3: countries that do not fully comply with minimum standards and are not making significant effort to do so and special cases - https://www.state.gov/reports/2024-trafficking-in-persons-report/

6 United States Department of the Treasury: Terrorist Assets Report (2020) -https://www.hsdl.org/c/abstract/?docid=858330; and

United States Department of State: Country Reports on Terrorism 2022 - https://www.state.gov/reports/country-reports-on-terrorism-2022/

7 United Kingdom's HM Treasury - https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases

8 TRACE Bribery Risk Matrix 2023 – countries with a risk score of 71 or more - https://www.traceinternational.org/trace-matrix

9 Transparency International: corruption perceptions index (2023) – countries with a score of 30 or less - https://www.transparency.org/en/cpi/2023

10 United States think-tank: Fund for Peace / Foreign Policy magazine: Fragile States Index (2024) – Top 40 countries - https://fragilestatesindex.org/global-data/

11 Global Terrorism Index 2024: Countries where the impact of terrorism is rated as being very high or high - https://www.visionofhumanity.org/maps/global-terrorism-index/#/

Index