Guernsey Financial Services Commission

Handbook on Countering Financial Crime and Terrorist Financing

June 2017 (Draft)

Contents

Table of Acronyms

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

ACDD	Additional Customer Due Diligence
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
CIS	Collective Investment Scheme
CMP	Compliance Monitoring Programme
EC	European Council
ECDD	Enhanced Customer Due Diligence
ESA	European Supervisory Authorities
EU	European Union
FATF	Financial Action Task Force
FCCO	Financial Crime Compliance Officer
FCRO	Financial Crime Reporting Officer
FIS	Financial Intelligence Service
FIU	Financial Investigation Unit
FSB	Financial Services Business
FT	Financing of Terrorism
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
LLP	Limited Liability Partnership
LP	Limited Partnership
LPP	Legal Professional Privilege
ML	Money Laundering
MONEYVAL	The Committee of Experts on the Evaluation of Anti-Money Laundering and the Financing of Terrorism
MVTS	Money or Value Transfer Service
NATO	North Atlantic Treaty Organization
NGCIS	Non-Guernsey Collective Investment Scheme
NO	Nominated Officer
NPO	Non-Profit Organisation
NRA	National Risk Assessment
NRFSB	Non-Regulated Financial Services Business
OECD	Organisation for Economic Co-operation and Development
OFAC	Office of Foreign Assets Control
PB	Prescribed Business

PC	Protected Cell
PCC	Protected Cell Company
PEP	Politically Exposed Person
PQ	Personal Questionnaire
PSP	Payment Service Provider
RFID	Radio-Frequency Identification
SAR	Suspicious Activity Report
SCDD	Simplified Customer Due Diligence
SDN	Specially Designated National
SIO	Senior Investigating Officer
SWF	Sovereign Wealth Fund
SWIFT	Society for Worldwide Interbank Financial Telecommunication
THEMIS	The FIS 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

Chapter 1
Introduction

Contents of this Chapter

1.1. Introduction

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

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

1.2. Background and Scope

(1) 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 Commission endorses the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation issued by the FATF. 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.

(2) Should the firm assist in laundering the proceeds of crime or in the financing of a terrorist act or organisation, it could face regulatory investigation, the loss of its reputation, and/or law enforcement investigation. The involvement of businesses with criminal proceeds or terrorist funds would also damage the reputation and integrity of the Bailiwick as an international finance centre.

(3) Under section 1(1) of 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 FT;
(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.

(4) The Bailiwick's AML and CFT 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.

(5) 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 the requirements of the FATF Recommendations are relevant to all businesses. This Handbook also recognises not only the differences between PBs and the financial services sector, but also the links between individual firms, particularly in the area of property transactions in some of the islands in the Bailiwick. Taking such an approach to the drafting of Schedule 3 and this Handbook helps to prevent the application of unnecessary and bureaucratic standards.

(6) In this regard, while the requirements of Schedule 3 and this Handbook (which provide for the undertaking of a risk-based approach, corporate governance, CDD, suspicion reporting, training and record keeping) apply equally to all firms, there are other requirements of Schedule 3 and this Handbook which may not be as relevant to some particular areas of industry. The application of these latter requirements will be dependant not only upon the assessed risk of the business itself but also upon the nature of the business undertaken.

1.3. Handbook Purpose

(1) 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: section 49AA(7) of the Law; paragraph 3(7) of Schedule 3 to the Law; section 15(8) of the Terrorism Law; section 15 of 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.

See Appendix B - Legislation

(2) This Handbook is issued to assist the firm in complying with the requirements of the relevant legislation concerning ML and FT, financial crime and related offences to prevent the Bailiwick's financial system and operations from being abused for ML and FT. 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.

(3) This Handbook has the following additional purposes:

(a) to outline the legal and regulatory framework for AML and CFT 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 and CFT 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 and FT and other financial crime.

1.4. The Bailiwick's AML and CFT Framework

(1) The Bailiwick's AML and CFT framework includes the following legislation (henceforth referred to as "the Relevant Enactments"):

(a) The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended ("the Law");
(b) The Drug Trafficking (Bailiwick of Guernsey) Law, 2000 as amended;
(c) The Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011 as amended ("the Terrorist Asset-Freezing Law");
(d) The Afghanistan (Restrictive Measures) (Guernsey) Ordinance, 2011;
(e) The Afghanistan (Restrictive Measures) (Alderney) Ordinance, 2011;
(f) The Afghanistan (Restrictive Measures) (Sark) Ordinance, 2011;
(g) The Al-Qaida (Restrictive Measures) (Guernsey) Ordinance, 2013;
(h) The Al-Qaida (Restrictive Measures) (Alderney) Ordinance, 2013;
(i) The Al-Qaida (Restrictive Measures) (Sark) Ordinance, 2014;
(j) The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 as amended ("the Terrorism Law");
(k) The Disclosure (Bailiwick of Guernsey) Law, 2007 as amended ("the Disclosure Law");
(l) The Transfer of Funds (Guernsey) Ordinance, 2017 ("the Transfer of Funds Ordinance");
(m) The Transfer of Funds (Alderney) Ordinance, 2017;
(n) The Transfer of Funds (Sark) Ordinance, 2017;
(o) The Disclosure (Bailiwick of Guernsey) Regulations, 2007 as amended;
(p) The Terrorism and Crime (Bailiwick of Guernsey) Regulations, 2007 as amended;
(q) The Registration of Non-Regulated Financial Services Businesses (Bailiwick of Guernsey) Law, 2008 as amended ("the NRFSB Law");

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

(2) Sanctions legislation is published by the States of Guernsey Policy and Resources Committee and can be accessed via the below website:

www.gov.gg/sanctions

1.5. Requirements of Schedule 3

(1) Schedule 3 includes requirements relating to:

(a) risk assessment and mitigation;
(b) undertaking CDD;
(c) monitoring customer activity and ongoing CDD;
(d) reporting suspected ML and FT activity;
(e) staff screening and training;
(f) record keeping; and
(g) ensuring compliance, corporate responsibility and related requirements.

(2) 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 and CFT 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.

1.6. Structure and Content of the Handbook

(1) 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 must 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.

(2) When obligations in Schedule 3 are explained or paraphrased in the Handbook the term 'shall' is used and reference is made to the relevant paragraph(s) of Schedule 3.

(3) Where the Commission Rules are set out, the terms 'must' is used and the text is presented in red shaded boxes for ease of reference.

(4) In both 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) as well as regulatory sanction and any other applicable sanctions.

(5) In respect of guidance, the Handbook uses the terms 'should' or 'may' to indicate ways in which the requirements of Schedule 3 and the Commission Rules can be satisfied, but allowing for alternative means of meeting the requirements.

(6) 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, good practice and amendments to Schedule 3 or the Relevant Enactments.

(7) This Handbook is not intended to provide an exhaustive list of appropriate and effective policies, procedures and controls to counter ML and FT. 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 and/or FT.

1.7. Significant Failure to Meet the Required Standards

(1) 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.

(2) 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.

(3) In addition, the Commission can take enforcement action under the Regulatory Laws for any contravention of the Commission Rules where the firm is licensed under one or more of those laws and/or under the Financial Services Commission Law.

(4) 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 NRFSB Law and the PB Law where the firm is registered with the Commission under those laws.

1.8. The Financial Action Task Force

(1) The FATF is an inter-governmental body 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, the financing of the proliferation of weapons of mass destruction and other related threats to the integrity of the international financial system.

(2) The FATF Recommendations are recognised as the global AML and CFT 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 the financing of proliferation of weapons of mass destruction;
(c) apply preventive measures for the financial sector and other designated sectors;
(d) establish powers and responsibilities for the competent authorities (e.g. investigative, law enforcement and supervisory authorities) and other institutional measures;
(e) enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and
(f) facilitate international co-operation.

1.9. The National Risk Assessment

(1) In accordance with the FATF Recommendations, the Bailiwick, led by the States of Guernsey Policy and Resources Committee, has conducted an NRA. The NRA adopts the IMF methodology and in this respect the relevant agencies within the Bailiwick have liaised closely with the IMF and industry to ensure a thorough assessment of the ML and FT risks the Bailiwick faces.

(2) The assessment of risks and vulnerabilities detailed within the NRA will naturally cascade through to specified businesses within the Bailiwick. In this regard, references are made throughout Schedule 3 and this Handbook requiring the firm to consider the content of the NRA when undertaking certain activities, e.g. the formulation of its business risk assessments and risk appetite.

(3) The Bailiwick will continue to review the NRA 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 through various surveys, regulatory returns and other statistical revenues.

(4) A copy of the Bailiwick's NRA can be found on the States of Guernsey Policy and Resource Committee's website:

National Risk Assessment (Awaiting Publication)

1.10 MONEYVAL

(1) 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 and FT and comply with the relevant international standards in these fields.

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

(3) MONEYVAL's most recent evaluation of the Bailiwick was conducted during October 2014 and assessed the Bailiwick's compliance with the FATF 2003 Recommendations. In its report, published on 15 January 2016, MONEYVAL concluded that the Bailiwick has 'a mature legal and regulatory system' and surpassed the equivalent review by the IMF in 2010.

Chapter 2
Corporate Governance

Contents of this Chapter

Schedule 3 Requirements

The requirements of Schedule 3 to the Law to which the Commission Rules and guidance in this chapter particularly relate are:

- Paragraph 12, which provides for the appointment of an FCRO and the reporting of suspicion.

  Paragraph 12 Hyperlink

- Paragraph 15, which makes provisions in relation to corporate governance and the review of compliance, including the requirement to appoint an FCCO.

  Paragraph 15 Hyperlink

2.1. Introduction

(1) Good corporate governance should provide proper incentives for the board and 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 and CFT obligations.

(2) The OECD describe 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 the framework for oversight of the policies, procedures and controls of the firm to counter ML and FT.

(5) References in this chapter and in the wider Handbook to "the board" must be read as meaning the senior management of the firm where the business is not a company, but is e.g. a partnership or a branch, or the natural person where a licence or registration is held in that person's own name.

2.2. GFSC Code of Corporate Governance

(1) The firm is expected to maintain good standards of corporate governance. In order to provide locally regulated financial services businesses 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").

The GFSC Finance Sector Code of Corporate Governance

(2) 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 regulated person's business without having to adhere to prescriptive rules.

(3) Whilst the Code does not apply to firms registered with the Commission under the NRFSB Law or the PB Law, the content can be used as a guide to the Commission's expectations when assessing compliance with this chapter by those businesses.

2.3. Board Responsibility for Compliance

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

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

(3) The board must organise and control the firm effectively, including establishing effective policies, procedures and controls as detailed below, and maintain appropriate resources to manage and mitigate the identified risks of ML and FT cost-effectively.

(4) Taking into account the conclusions of the business risk assessments, in accordance with paragraph 2 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.

(5) 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, covering all aspects of the firm and its operations, to identify the inherent ML and FT risks and to define the firm's AML and CFT risk appetite (see chapter 3);
(b) risk assess all customers to identify: 1) those to which ACDD and/or ECDD measures and monitoring must be applied; and 2) those customers for which SCDD measures can be taken where the firm considers this appropriate (see chapter 3);
(c) identify and verify customers, including natural persons, legal persons and legal arrangements (see chapters 4-7);
(d) identify customers to an extent sufficient to establish: 1) the beneficial owners and underlying principals; and 2) the purpose and intended nature of the business relationship or occasional transaction (see chapters 4-7);
(e) undertake sufficient CDD to validate why the customer (including the beneficial owner and underlying principal) is using the firm's products and services and that these reasons are consistent with the firm's understanding of the rationale for the arrangement (see chapters 4-7);
(f) apply ECDD measures to those customers deemed to pose a high risk of ML and/or FT, sufficient to mitigate any specific risks arising (see chapter 8);
(g) apply ACDD measures where the customer falls within the categories listed in paragraph 5(2) of Schedule 3 (see chapter 5);
(h) apply SCDD measures in an appropriate manner where the circumstances of a business relationship or occasional transaction are such that the ML and FT risks have been assessed as low (see chapter 9);
(i) conduct transaction and activity monitoring (see chapter 11);
(j) 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);
(k) screen customers, beneficial owners and underlying principals at an appropriate frequency to enable the prompt identification of any natural or legal persons subject to UN, EU or other sanction (see chapter 12);
(l) report promptly to the FIS where the firm knows or suspects, or has reasonable grounds for knowing or suspecting, that a customer or potential customer (including an attempted transaction) is involved in ML and/or FT (see chapter 13);
(m) screen transfers of funds for missing or incomplete payer and payee information where the firm is a PSP (see chapter 14);
(n) screen potential employees to ensure the suitability, probity and competence of board and staff members (see chapter 15);

(o) provide suitable and sufficient AML and CFT training to all relevant employees and identify those employees to whom additional training must be provided and provide such additional training (see chapter 15);
(p) 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);
(q) ensure that where the firm is a majority owner or exercises control over a branch or subsidiary established outside the Bailiwick, that the branch or subsidiary applies controls consistent with the requirements of Schedule 3 or requirements consistent with the FATF Recommendations; and
(r) ensure that measures are in place to effectively share CDD and other information between the firm and its majority owned subsidiaries and branches over which it exercises control.

(6) More information on the process and requirements for conducting business risk assessments can be found in chapter 3 of this Handbook.

Risk Based Approach

2.4. Board Oversight of Compliance

(1) The board is responsible for establishing and maintaining a policy, including a monitoring programme, for the firm to review its compliance with the requirements of Schedule 3 and the Commission Rules.

(2) 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 any 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 firm must make those changes.

(3) As part of its compliance arrangements, the board is responsible for appointing an FCCO, the function of which is to have oversight of the firm's compliance with its obligations under Schedule 3 and the Commission Rules. This section should therefore be read in conjunction with section 2.8. of this Handbook which sets out the roles and responsibilities of the FCCO.

Financial Crime Compliance Officer

(4) In addition to appointing an FCCO, the board of the firm must consider periodically whether, based upon the size and risk profile of the firm, whether it would be appropriate to maintain an independent audit function to test the ML and FT policies, procedures and controls of the firm.

(5) The board must ensure that the compliance review policy 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.

(6) 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, ACDD and SCDD;
(b) the management information received by the board, including information on any branches and subsidiaries;

(c) the management and testing of third parties upon which reliance is placed for CDD, including introducer relationships together with outsourcing arrangements;
(d) the ongoing competence and effectiveness of the FCRO;
(e) the handling of SARs, disclosures and any production orders or requests for information from the FIS;
(f) the management of sanctions risks and the handling of sanctions notices;
(g) the provision of AML and CFT 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, e.g. gifts and hospitality policies and registers.

(7) The board may delegate some or all of its duties but must retain responsibility for the review of overall compliance with the AML and CFT requirements of Schedule 3 and the Commission Rules.

(8) Where the firm identities 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 Rule 2.7.(1) of this Handbook where the deficiencies identified are considered to be serious or material.

(9) In respect of a managed or administered firm, the responsibility for the firm and its compliance with Schedule 3 and the Commission Rules is retained by the board and senior management of the managed or administered firm and not transferred to the manager or administrator of that firm.

2.5. Outsourcing

(1) 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 and the Commission Rules. The firm cannot contract out of its statutory and regulatory responsibilities to prevent and detect ML and FT.

(2) Where the firm is considering the outsourcing of functions to a third party, the firm should:

(a) consider and adhere to 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; and
(d) ensure that the board, the FCRO, other third parties and all employees understand the roles, responsibilities and respective duties of each party.

(3) 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 POI Law and the Banking Law respectively, the principles contained within are relevant across industry and provide a useful reference when considering an outsourcing arrangement:

Guidance Note on the Outsourcing of Functions by Entities Licensed under the POI Law
Outsourcing Risk Guidance Note for Banks

(4) Prior to a decision being made to establish an outsourcing arrangement, the firm must make an assessment of any potential risk exposure to ML and FT and must maintain a record of that assessment, either as part of its business risk assessments or within a separate outsourcing risk assessment.

(5) The firm should monitor the perceived risk(s) identified by its assessment of an outsourcing arrangement and review this risk assessment on an on-going basis in accordance with its business risk assessment obligations.

(6) The firm should ensure, at the commencement of an outsourcing arrangement and on an ongoing basis, that:

(a) the outsourced service provider is appropriately qualified, knowledgeable of the applicable AML and CFT requirements and sufficiently resourced to perform the required activities;
(b) the outsourced service provider 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 and FT risks;
(c) the outsourced service provider is screened and subject to appropriate due diligence in accordance with this Handbook to ensure the probity of the outsourced service provider;
(d) the work undertaken by the outsourced service provider is monitored to ensure it complies with the requirements of Schedule 3 and/or the Commission Rules;
(e) 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
(f) 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.

(7) The fact that the firm has relied upon an outsourced service provider or the report of an outsourced service provider will not be considered to be a mitigating factor where the firm has failed to comply with the requirements of Schedule 3 and/or the Commission Rules. The board should therefore ensure the veracity of any reports provided by an outsourced service provider, e.g. by spot checking aspects of such reports.

(8) 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 and/or FT activity in connection with the outsourcing firm's business will be reported by the outsourced service provider to the FCRO of the outsourcing firm in a timely manner.

(9) An exception to Rule 2.7.(7) would be where the outsourced service provider forms a suspicion that the outsourcing firm is complicit in ML and/or FT activity. In such cases the outsourced service provider, where it is a specified business, must disclose its suspicion to the FIS in accordance with chapter 13 of this Handbook and advise the Commission of its actions in accordance with Rule 2.7.(1).

(10) Where the firm chooses to outsource or subcontract work to a non-regulated entity, it should bear in mind that it remains subject to the obligation to maintain appropriate policies, procedures and controls to prevent ML and FT. In this context, the firm should consider whether the subcontracting increases the risk that it will be involved in, or used for, ML and/or FT, in which case appropriate and effective controls to address that risk should be implemented.

2.6. Foreign Branches and Subsidiaries

(1) Where the firm has any branch offices, majority-owned subsidiary companies, or otherwise directly or indirectly exercises control over an FSB or PB in any country or territory outside the Bailiwick, the firm must ensure that its AML and CFT compliance arrangements and programmes are applied to the business of those branch offices, subsidiaries or other entities.

(2) In determining whether the firm exercises control over another entity, examples could include one or more of the following: where the firm determines appointments to the board or senior management of a group company; where the firm determines the group company's business model or risk appetite; and/or where the firm is involved in the day-to-day management of the group company.

(3) The AML and CFT programmes should incorporate the measures required under Schedule 3, should be appropriate to the business of the branch offices, majority-owned subsidiaries and other entities and should be implemented effectively at the level of those entities.

(4) The AML and CFT programmes should incorporate policies, procedures and controls for sharing information required for the purposes of CDD and ML and FT risk management. In this respect, group-level compliance, audit and/or AML and CFT functions should be provided with, or have access to, information about customers, accounts and transactions from branch offices and majority-owned subsidiaries when necessary for AML and CFT purposes.

(5) The firm must ensure that adequate safeguards on the confidentiality and use of information exchanged are in place between group entities.

(6) Where a branch office or majority-owned subsidiary is unable to observe the appropriate AML and CFT measures because local laws, regulations or other measures prohibit this, Schedule 3 requires that the firm inform the Commission. The firm should also ensure that appropriate controls are implemented to mitigate any risks related to the specific areas where compliance with appropriate AML and CFT measures cannot be met.

(7) The firm must be aware that this inability to observe the appropriate AML and CFT 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 and FT risks associated with conducting business in such a country or territory.

2.7. Liaison with the Commission

(1) The board of the firm must ensure that the Commission is advised of any material failure to comply with the provisions of Schedule 3 or the Commission Rules, or of any serious breaches of the policies, procedures or controls of the firm.

(2) 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 (e.g. 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 is aware that an aspect of material non-compliance may have occurred across more than one member of a corporate group of which it is a member;
(d) the firm discovers that the party to whom it has outsourced functions critical to compliance with Schedule 3 and this Handbook has failed to apply one or more of the requirements of Schedule 3 and/or Commission Rules and remediation work is required;
(e) any aspect of material non-compliance identified involving any country listed in the Commission's Business from Sensitive Sources Notices, regardless of the number of business relationships/occasional transactions or values involved; or
(f) 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,

(3) In addition to the above, the Commission would expect to be advised where the firm identifies a breakdown of administrative or control procedures, e.g. 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 and/or this Handbook.

(4) The Commission recognises that from time to time the firm may identify instances of non-compliance as part of its ongoing monitoring or customer risk 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 due diligence held for the customer, beneficial owner and underlying 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 relationship.

(5) 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.

(6) 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.

(7) While not an exhaustive list, the following are examples of what the Commission considers to constitute poor practice in relation to the failure to notify it under Rule 2.7.(1) of this Handbook:

(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) there is 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. Financial Crime Compliance Officer

(1) In accordance with paragraph 15(1)(a) of Schedule 3, the firm shall appoint a person of at least management level as the FCCO and appoint a replacement to fill this position if it becomes vacant. The firm should provide the name of the FCCO to the Commission within 14 days starting from the date of that person's appointment. Notification should be made via the Commission's PQ Portal:

https://online.gfsc.gg

(2) The FCCO appointed by the firm must:

(a) be a natural person;
(b) be of at least management level;
(c) be appropriately qualified 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 FCCO); and
(e) be resident in the Bailiwick.

(3) The firm must ensure that the FCCO:

(a) is appropriately independent from the day-to-day business of the firm, in particular any customer-facing or business-development roles;
(b) has timely and unrestricted access to the records of the firm;
(c) has sufficient resources to perform his duties;
(d) has the full co-operation of the firm's staff;
(e) is fully aware of his obligations and those of the firm; and
(f) 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 and this Handbook are being met and that the firm is taking sufficiently robust measures to protect itself against the potential risk of being used for ML or FT.

(4) The primary role of the FCCO is to have oversight of the firm's compliance with its obligations under Schedule 3, the Commission Rules and the Relevant Enactments. As such the functions of the FCCO include:

(a) having oversight of the monitoring and testing of AML and CFT 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 its attention; and
(e) acting as a point of contact with the Commission and to respond promptly to any requests for information made.

(5) While it is not anticipated that the FCCO will conduct all monitoring and testing himself, the expectation is that the FCCO will have oversight of any monitoring and testing being conducted by the firm, e.g. by a compliance team or an outsourcing oversight team, in accordance with the firm's compliance review policy.

(6) With regard to Rule 2.8.1.(3)(a), the appropriateness of the FCCO's independence should be determined based upon the size, nature and complexity of the firm's operation. In this respect the circumstances may be such that, due to the number of persons employed by the firm, the FCCO holds additional functions or is responsible for other aspects of the firm's operation.

(7) Where the FCCO holds additional functions or is responsible for other aspects of the firm's operation, the firm should ensure that those additional functions or responsibilities are subject to appropriate oversight, e.g. by an independent auditor or member of the board, or are subject to periodic independent scrutiny.

(8) For the avoidance of doubt, the same individual can be appointed to the positions of FCRO and FCCO, 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. Financial Crime Reporting Officer

(1) In accordance with paragraph 12(a) of Schedule 3, the firm shall appoint a person of at least management level as the FCRO and appoint a replacement to fill this position if it becomes vacant. The firm shall provide the name of the FCRO to the Commission within 14 days from the date of that person's appointment. Notification should be made via the Commission's PQ Portal:

https://online.gfsc.gg

(2) The FCRO appointed by the firm must:

(a) be a natural person;
(b) be of at least management level;
(c) be appropriately qualified;
(d) be employed by 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 FCRO); and
(e) be resident in the Bailiwick.

(3) The firm must ensure that the FCRO:

(a) is the main point of contact with the FIS in the handling of disclosures;
(b) has unrestricted access to the CDD records of the firm's customers;
(c) has sufficient resources to perform his 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 personal obligations and those of the firm under Schedule 3, the Commission Rules and the Relevant Enactments.

(4) The firm must provide the FCRO with the authority to act independently in carrying out his responsibilities under part 1 of the Disclosure Law or section 15 or 12 of the Terrorism Law. The FCRO must be free to have direct access to the FIS in order that any suspicious activity may be reported as soon as is practicable. The FCRO must also be free to liaise with the FIS on any question of whether to proceed with a transaction in the circumstances.

2.8.3. Nominated Officer

(1) In order to meet the requirements of paragraph 12(b) or 12(c) of Schedule 3, the firm must nominate at least one other natural person to receive disclosures in the absence of the FCRO.

(2) The NO(s) must:

(a) be a natural person; and
(b) be appropriately qualified.

(3) There is no obligation to advise the Commission of the details of the NO(s) and in this regard no Form PQ is required. However, were the NO is acting in place of the FCRO to cover an extended period of absence, e.g. maternity leave, sabbatical or long-term sick leave, the firm should consider appointing the NO as the FCRO on a temporary basis. Where this occurs, a notification should be made to the Commission in accordance with paragraph 2.8.2.(1) above.

(4) The firm must communicate the name of the NO(s) to the employees of the firm and ensure that all employees of the firm are aware of the natural person(s) to whom SARs are to be made in the absence of the FCRO.

(5) For the avoidance of doubt, this requirement does not apply to sole traders, such as personal fiduciary licence holders and natural persons registered as PBs in their own name.

Chapter 3
Risk Based Approach

Contents of this Chapter

Schedule 3 Requirements

The requirements of Schedule 3 to the Law to which the Commission Rules and guidance in this chapter particularly relate are:

- Paragraph 2, which provides an over-arching duty on a specified business to understand, assess and mitigate the risks of ML and FT to its business.

  Paragraph 2 Hyperlink

- Paragraph 3, which provides for a specified business to identify and assess the risks of ML and FT, both in respect of its business as a whole and its individual business relationships or occasional transactions. Schedule 3 also provides for a firm to ensure that its policies, procedures and controls are effective and appropriate to the assessed risk.

  Paragraph 3 Hyperlink

- Paragraph 14, which provides for the record keeping requirements of a specified business.

  Paragraph 14 Hyperlink

- Paragraph 15, which makes provisions in relation to corporate governance and the review of compliance, including the requirement to appoint an FCCO.

  Paragraph 15 Hyperlink

3.1. Introduction

(1) This chapter, together with Schedule 3, 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 and FT. The chapter is broken down into three main segments:

(a) Risk Based Approach - which provides a high-level overview of the risk based approach;
(b) Business Risk Assessments - which details the Commission Rules and guidance in respect of the firm's ML and FT risk assessments; and
(c) Customer Risk Assessment - which sets out the Commission Rules and guidance for the conducting of customer risk assessments.

3A. Risk Based Approach

3.2. Definition, Purpose and Benefits

(1) A risk-based approach towards the prevention and detection of ML and FT aims to support the development of preventative and mitigating measures that are commensurate to the ML and FT risks identified by the firm and to deal with those risks in the most cost-effective and proportionate way.

(2) In this respect a risk-based approach uses five steps to deal with the ML and FT risks faced by the firm:

(a) identifying the specific threats posed to the firm by ML and FT and those areas of the business with the greatest vulnerability;
(b) assessing the likelihood of those risks occurring and the impact of such on the business;
(c) reviewing and monitoring those risks to identify changes in the threats posed to the firm;
(d) mitigating the likelihood of occurrence and the potential damage that can be caused, primarily through the application of appropriate and effective policies, procedures and controls; and
(e) managing the residual risks, threats and vulnerabilities that the firm has been unable to mitigate.

(3) 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.

(4) 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 and FT, taking into account its customers, products and/or services and the ways in which it provides those products and/or services.

(5) In determining how the risk-based approach should be implemented, the firm should analyse and seek to understand how the identified ML and FT risks affect its business. This determination should take into account a range of inputs, including amongst other things the firm's appetite for risk, its AML and CFT experience and the Bailiwick's NRA.

(6) 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 and FT risks. It should be noted however that a risk-based approach does not exempt the firm from the requirement to apply enhanced measures when it has identified higher risk situations.

(7) Schedule 3 and this Handbook do not prohibit the offering of any products or services or the acceptance of any customers, unless they are undertaking ML and/or FT. The risk-based approach, as defined in Schedule 3 and this Handbook, instead requires that the risks posed by customers, products and services are identified, managed and mitigated and that evidence of such is documented and reviewed on an on-going basis.

(8) By adopting a risk-based approach the firm should ensure that measures to prevent or mitigate ML and FT 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.

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

(10) The benefits of a risk-based approach include:

(a) recognising that the ML and FT threats to the firm vary across its customers, countries/territories, 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 and/or FT occurring;
(e) reflecting experience and proportionality through the tailoring of effort and activity to risk;
(f) enabling the application of the requirements in this Handbook sensibly and in consideration of all relevant risk factors;
(g) allowing for the consideration of the accumulation of identified risks and the determination of the level of overall risk and the appropriate level of mitigation to be applied; and
(h) differentiating the extent of measures, depending on the type and level of risk for the various risk factors (e.g. in a particular situation, it is possible to apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa).

(11) It is important to realise and understand 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 and FT that is appropriate in one sector may be inappropriate in another.

3.3. Identification and Mitigation of Risks

(1) 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 people, 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 and FT may cause.

(2) Having identified its threats and vulnerabilities, 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 relation to a particular part of the firm 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.

(3) In accordance with subparagraph 3(7) of Schedule 3, the firm shall have regard to:

(a) any relevant rules and guidance in this Handbook;
(b) any relevant notice or instruction issued by the Commission under the Law; and
(c) the current version of the NRA

when determining what constitutes high and low risk when undertaking business and customer risk assessments, and what constitute appropriate measures to manage and mitigate risks for the purposes of the firm's policies, procedures and controls.

(4) Retaining documentation on the results achieved through 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 and FT;
(b) agrees and implements appropriate and effective policies, procedures and controls to manage and mitigate ML and FT 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 Risks

(1) In addition to the individual consideration of each stand-alone risk identified within the firm's business risk assessments, the firm must consider the cumulative effect of a combination of two or more of those risks and the dynamic that this could have on the controls implemented by the firm to mitigate those risks. In this regard, the firm must consider not only each of the ML and FT risks individually, but also whether their concurrent or cumulative effect might raise the firm's overall risk exposure.

(2) Such an approach is relevant not only to the firm in its consideration of the risks posed to the business as a whole, but also in the consideration of individual customer risk.

(3) There are also other operational factors which may increase the overall level of risk. These risks should be considered parallel to, or in combination with, the firm's ML and FT risks. Examples of such could be the outsourcing of AML and CFT controls or other regulatory requirements to an external third party or another member of the same group of companies 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.

3B. Business Risk Assessments

3.5. Introduction

(1) 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 and FT 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.

(2) 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 the business and its products and services are exposed to ML and FT. Good business risk assessments are therefore vital for ensuring that the firm's policies, procedures and controls are proportionate and targeted appropriately.

(3) The format of the business risk assessments is a matter to be decided by the firm; however, regardless of the format used, the firm must ensure that its business risk assessments are documented in order to be able to demonstrate the basis upon which it has been conducted.

3.6. Content and Structure of Business Risk Assessments

(1) In accordance with paragraph 3 of Schedule 3, the firm shall undertake risk assessments of both the ML and FT risks faced by the firm. These assessments shall be suitable, sufficient and 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.

(2) Notwithstanding the requirement for the assessments to be distinct, there is nothing to prevent them being contained within one over-arching document recording the firm's business risk assessments, together with any other risk assessments (i.e. a technology risk assessment), for record keeping purposes.

(3) As a minimum the firm's business risk assessments must assess the ML and FT risks posed by the following areas:

- (a) the nature, scale and complexity of the firm's activities;
- (b) the products, services and transactions provided, or facilitated, by the firm;
- (c) the countries and geographic areas associated with the business of the firm (e.g. the countries and geographic areas into which the firm markets its products and services; the countries and geographic areas from which its customers emanate etc.);
- (d) the customers to whom the products and services are provided;
- (e) the manner in which the products and services are provided (delivery channel);
- (f) the use of any third parties through outsourcing/introducer arrangements or similar;
- (g) the use of technology in its products and services and any developments in the technologies used; and
- (h) an assessment of the cumulative effect that the presence of more than one risk variable may have.

(4) The business risk assessments must also reflect the firm's assessment of whether the risks identified in the NRA are relevant or potentially relevant to the firm, and where so, identify the measures for mitigating those risks.

(5) In addition to identifying any particular areas of vulnerability to the risks of ML and FT, 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.

(6) Industry sectors will have inherent and/or generic risk factors and these should be referenced. Additionally, the firm will also have risk factors particular to its own business which should be analysed in the business risk assessments.

(7) The firm must not copy the risk assessments prepared by another business, or use 'off-the-shelf' assessments which pre-identify suggested ML and FT risks. Such an approach can lead to the firm failing to accurately identify the ML and FT risks specific to its business, in turn leading 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.

(8) 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. This does not demonstrate that the board has given serious consideration to the vulnerabilities particular 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, e.g. 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; or
(d) focus upon isolated risk factors, e.g. concentrating solely upon a geographic location.

(9) There may be occasions where threats span a number of risk categories, e.g. there may be operational risks associated with a piece of client-facing technology as well as ML and FT or other financial crime risks. Where the firm wishes to combine its ML and FT risk assessments with conduct, credit or other business risk assessments, the firm should ensure that the assessment of each risk is clearly identified.

3.7. Risk Appetite and Tolerance

(1) As part of its business risk assessments the firm must include a risk appetite statement which clearly sets out the type and extent of the risks that the firm is willing to accept, or to avoid, in order to achieve its strategic business objectives.

(2) 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 statement 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.

(3) The risk appetite statement should include a qualitative statement as well as quantitative measures to support its risk appetite, including the firm's 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.

(4) The board must ensure that the risk appetite statement is communicated to all relevant employees. It should also ensure that employees understand the risk appetite and its effect on the strategic objectives of the firm, in particular those employees with customer-facing or business development roles.

(5) The following are examples of questions the firm should consider in developing its risk appetite:

(a) What are the strategic objectives of the firm? Are they clear?
(b) What is explicit and what is implicit in those objectives?
(c) What are the significant risks the board is willing to take?
(d) What are the significant risks the board is not willing to take?

(e) Is the board clear about the nature and extent of the significant risks it is willing to take in achieving its strategic objectives?
(f) Have the board and management team reviewed the capabilities of the firm to manage the risks that it faces?
(g) What capacity does the firm have in terms of its ability to manage risks?
(h) Do employees of the firm understand their role and responsibility for managing risk?
(i) 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?
(j) Does the firm understand clearly why and how it engages with risks?

3.8. Business Risk Assessments Review

(1) Just as the activities of the firm can change, so too do the corresponding ML and FT 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. Any such changes will result in a need for a review of the business risk assessments to be conducted to ensure that the controls to mitigate those risks remain effective.

(2) Other operational changes, such as a change in staffing numbers or a change to group policies, can all have an impact upon the resources required to effectively manage ML and FT risks.

(3) The board of the firm must regularly review its ML and FT business risk assessments so as to ensure they remain current. Such reviews must be conducted at a minimum annually, or whenever any material change to the business of the firm occurs.

(4) Where, as a result of the review undertaken, the board determines that changes to the business risk assessments are required, it must ensure that such changes are made and give consideration to whether the policies, procedures and controls of the firm remain appropriate and effective in light of the revised assessments, making any changes it considers appropriate.

3.9. Example Risk Factors

(1) Below are example risk factors that may be considered by the firm as part of the assessments of its ML and FT risks. The below lists are provided purely as examples and are not intended to be exhaustive or used by the firm as a checklist of risks.

(2) Customer risk:

(a) the geographical origin of customers;
(b) the complexity of customer structures;
(c) the complexity of legal persons and legal arrangements;
(d) the use of introduced business arrangements;
(e) the use or acceptance of omnibus or pooled accounts;
(f) the number of customers assessed as high risk;
(g) the countries and territories from which the firm will accept customers; and
(h) the number of customers assessed as PEPs and their associated jurisdictions.

(3) Product/service risk:

(a) the nature, scale, diversity and complexity of the products and services of the firm;
(b) the target markets, both in terms of geography and class of customer;

(c) the distribution channels utilised by the firm;
(d) whether the value of transactions is expected to be particularly high;
(e) whether payments to third parties are allowed; and
(f) whether the products/services/structure is of particular, or unusual, complexity.

(4) Other potential sources of risk to consider:

(a) internal and/or external audit findings; and
(b) typologies and findings of ML and FT case studies.

3.10. New Products and Practices

(1) In accordance with subparagraph 3(3)(c)(i) of Schedule 3, the firm must, prior to adopting or making available new business practices, products or services, have identified and assessed the ML and FT risks and vulnerabilities arising from those products, services or practices and documented those risks.

(2) Any risk assessment of a new business practice, product or service undertaken in accordance with Rule 3.10.(1) above can either be documented as a standalone risk assessment or be included within the firm's wider ML and FT risk assessments.

(3) If the firm decides to proceed with the adoption or offering of a new business practice, product or service, the board of the firm must approve the risk assessment and that approval must be documented.

3.11. New Technologies

(1) In accordance with subparagraph 3(3)(c)(ii) of Schedule 3, the firm must, prior to adopting and using a new or developing technology, have identified and assessed the ML and FT risks and vulnerabilities arising from its use or adoption and documented these risks.

(2) Any risk assessment of new or developing technology adopted or used by the firm can either be conducted as a standalone risk assessment or included within the firm's wider ML and FT business risk assessments. This includes new or developing technologies in both the Financial Technology ("FinTech") and Regulatory Technology ("RegTech") arenas, though the content and focus of the assessments will differ depending on whether the technology is used within the firm's financial services products or services, its delivery channels, or in business processes such as customer take-on.

(3) It should be borne in mind that the risks presented by FinTech and RegTech differ. In contrast to the largely customer-facing FinTech products and services, the majority of RegTech operates in support of a firm's middle and back-office operations. In this respect, while RegTech can also present risks to the firm, those risks are likely to present themselves differently and require different methods of management and mitigation.

(4) The requirements of subparagraph 3(3)(c)(ii) of Schedule 3 and Rule 3.11.(1) of this Handbook apply to the adoption of FinTech and RegTech technologies which significantly impact upon the AML and CFT controls of the firm, and not to minor technologies used to support the day-to-day running of the business, e.g. anti-virus software, office tools etc. In this respect, the focus of the firm should be on those technologies which expose the firm to the greatest risk of financial crime, including its susceptibility to being used for ML or to facilitate FT. Examples of such technologies include customer-facing portals or other software where customers can interact with the firm, e.g. online trading platforms, banking applications or mobile payment solutions.

(5) On an ongoing basis the firm must periodically review any risk assessments of new or developing technology in conjunction with its responsibility for the review of its ML and FT risk assessments as described in section 3.8. of this Handbook.

(6) While the firm must review its assessment of any new or developing technology on an ongoing basis, such risk assessment need only be updated when significant changes to the technological product or system are implemented.

3.11.1. Technology Risk Assessment Content and Scope

(1) The risk assessment of a new or developing technology must include, as a minimum, an assessment of the risks and vulnerabilities inherent in the system in order that appropriate controls can be implemented to minimise the opportunity for the abuse of the technology. This includes evaluating:

(a) the technology itself;
(b) the provider of the technology and any other connected third parties; and
(c) the anticipated use of the technology and the threats posed by this use.

(2) It is not essential that the risk assessment of a technology extends to a highly technical comprehensive report on the specifications and functionality. The objective of the risk assessment is to evaluate the ML and FT risks and vulnerabilities inherent in the use of the technological method or system and to identify the controls necessary to mitigate and limit the firm's exposure.

(3) The following are examples of points to consider when undertaking a risk assessment of a new or developing technology. The examples given below are not exhaustive of every factor for consideration and they are not proposed as a checklist. The guidelines detail a wide range of factors that could be considered in order to cater for the different types of technological products, methods or systems the firm might contemplate using. It is acknowledged that in some instances the firm may elect to use alternative or a limited number of the factors listed due to the technology being implemented.

(4) The technology:

(a) What are the security controls inherent in the system?
    (i) What are the levels of user security and accessibility?
    (ii) Are there adequate controls regarding the security of data?
(b) How are updates to the technology issued?
    (i) How does the firm monitor the security of those channels?
(c) How will the technology interact with the firm's current IT systems and infrastructure?
(d) Do the firm's existing fraud prevention, AML and CFT policies, procedures and controls need realignment or require amendment to accommodate process changes introduced through the use of the technology?
    (i) Where the technology provides for remote access by customers, how will the firm manage the additional risks arising from this?
(e) Is it necessary to obtain customer consent in order to obtain, research or retain data? Have these requirements been reflected within the relevant processes?
(f) How does the firm corroborate any information provided by the technology and is it acceptable to the firm?
(g) How has the firm satisfied itself that the requirements of Schedule 3, the Commission Rules and the Relevant Enactments continue to be met following the introduction of the technology?
    (i) Are there mechanisms in place to ensure consistency with any future changes in international standards and requirements?

(5) The provider (and other connected third parties):

(a) If an external provider is used, is there transparency of the methodologies used by the provider?
(b) Is there a capability to cancel any arrangement with an external provider?
(i) If so, does the firm have sufficient knowledge and resources to continue utilising and supporting the technology in a safe and effective manner?
(c) Where the technology gathers data or documentation, who owns it and where is it stored?
(d) If the provider of the product or system or a third party retains the data and documentation, is there a contract or contingency plan to recover any data in the event of any changes occurring in the relationship with the provider?
(e) What controls does the firm have in place for an unexpected event in respect of the provider or third party, i.e. a natural or other disaster affecting the capability of the provider, or its closing/winding-up?

(6) The anticipated use:

(a) Have staff been given appropriate training to understand the technology and the boundaries of what is expected from their or the customer's interaction with the technology?
(b) Are there controls in place to alert the firm where unexpected activity occurs within the system, i.e. multiple remote-access attempts across customers, denial of service attacks, etc.?
(c) Are there procedures in place to mitigate any risks arising where security or other operational issues are identified within the technology to mitigate any threat to the firm or its customers?
(i) How will the firm manage the reputational risks arising from such incidents?

3C. Customer Risk Assessment

3.12. Introduction

(1) The purpose of this section is to set out the rules and guidance surrounding the risk assessment of new customers at the point of take-on, as well as the ongoing requirements to ensure that any risk assessment remains appropriate and relevant as the relationship with the customer evolves.

(2) 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 customer against the parameters determined within the risk appetite and the ML and FT risks identified in the business risk assessments.

(3) There may be circumstances where the risks of ML and FT are higher and ECDD measures are to be taken. Similarly there are a small number of circumstances within which the firm can apply SCDD measures because the risk of the business relationship or occasional transaction has been assessed as low. Further information on the risk assessment process, including examples of high and low risk characteristics, can be found in this section.

3.13. Management and Mitigation

(1) In order to consider the extent of its potential exposure to the risks of ML and FT, in accordance with paragraph 3(4)(a) of Schedule 3 the firm shall undertake an assessment of the risk of a proposed business relationship or occasional transaction prior to the establishment of that relationship or the carrying out of an occasional transaction. Based on the outcome of that

assessment, the firm should decide whether or not to accept the business relationship or whether or not to carry out an occasional transactions.

(2) When assessing the risk of a proposed business relationship or occasional transaction the firm must ensure that all relevant risks are considered, both singly and in combination, before making a determination as to the level of overall assessed risk.

(3) When undertaking a customer risk assessment the firm must take into consideration, as a minimum, the following:

(a) the type and identity of the customer, and any beneficial owner and underlying principal;
(b) the identity of any beneficiaries (including beneficiaries of a life policy);
(c) the associated countries or territories;
(d) the products, services and transactions being provided or facilitated;
(e) the delivery channels through which those products and/or services are being provided;
(f) 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 arrangement;
(g) the type, volume, value and regularity of activity expected;
(h) the expected duration (if a business relationship); and
(i) whether cumulatively these factors increase or decrease the potential risk.

(4) Consideration of the purpose and intended nature of a business relationship or occasional transaction in accordance with Rule 3.13.(3)(f) should include an assessment of the economic or other commercial rationale for the business relationship or occasional transaction.

(5) Based upon the results of the customer risk assessment, the firm must determine, on a risk-based approach, the extent of the identification information, including CDD, ACDD and ECDD (as applicable), to be obtained in accordance with paragraphs 4 and 5 of Schedule 3; how that information will be verified; and the extent to which the resulting business relationship will be monitored on an ongoing basis.

3.14. Procedures and Record Keeping

(1) The firm's policies, procedures and controls towards the identification and assessment of risk in its customer base must be appropriate, effective, documented and approved by the board.

(2) The firm's policies, procedures and controls must be sufficiently detailed to allow it to demonstrate how the assessment of each business relationship or occasional transaction has been reached and which take into account the nature and complexity of the firm's operation.

(3) The procedures may provide for standardised profiles to be used 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.

(4) 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 assessment of risk of that customer has been made, assessing each risk factor/variable on a singular basis, as well as the cumulative effect of those risk factors/variables.

(5) Where, despite there being high risk factors or variables 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 customer file.

3.15. Business from Sensitive Sources Notices, Instructions, etc.

(1) From time to time the Commission issues Business from Sensitive Sources Notices, Advisory Notices, Instructions and Warnings which highlight potential risks arising from particular countries and territories. The information contained within these notices, together with sanctions legislation applicable in the Bailiwick, must be considered when undertaking a relationship risk assessment.

Business from Sensitive Sources Notices

(2) Further information on the Bailiwick's sanctions regime and legislation can be found in chapter 12 of this Handbook.

UN, EU and Other Sanctions

3.16. Mandatory High Risk Factors

(1) A customer which exhibits one or more of the following characteristics must be rated as high risk and ECDD measures must be applied in the due diligence process for that customer as set out in chapter 8 of this Handbook:

(a) the customer, or any beneficial owner or underlying principal, is a foreign PEP;
(b) the customer is established or situated in a country or territory which has been identified by credible sources, such as mutual evaluations, detailed assessments or published follow-up reports, as having not applied or insufficiently applied the FATF Recommendations (see Part A of the Business from Sensitive Sources Notices issued by the Commission from time to time);
(c) the customer is established or situated in a country or territory which is of concern to the Commission (see Part C of the Business from Sensitive Sources Notices issued by the Commission from time to time);
(d) the customer is established or situated in a country or territory identified by credible sources as providing funding or support for terrorist activities;
(e) the customer is established or situated in a country or territory otherwise identified by the FATF as a country for which ECDD measures are appropriate; or
(f) a correspondent banking relationship or similar relationship involving the provision of services, which themselves amount to financial services business or facilitate the carrying on of such business, by one FSB to another.

3.17. Potential High Risk Indicators

(1) The risk indicators included within the following sections are purely guidance and provided as examples of risk factors that the firm might consider when undertaking a risk assessment of a business relationship or occasional transaction. The lists are not definitive and they are not prescribed as checklists. It is for the firm to assess and decide what is appropriate in the circumstances of the customer and the example indicators do not diminish or remove the ability of the firm to apply a risk-based approach.

(2) If it is determined through a risk assessment that there are types of customer, activity, business or profession that are at risk of abuse from ML and/or FT then the firm should apply higher AML and CFT requirements to such sectors.

3.17.1. Geographic – Connected Countries or Territories

(1) A customer with a connection to a country or territory:

(a) with known higher levels of bribery and corruption;
(b) with known higher levels of organised crime;
(c) involved in illegal drug production, processing and/or distribution; or
(d) with known higher levels of other criminal activity;

other than those countries or territories falling within points (b) and (c) in Rule 3.16.(1) above where a mandatory high risk rating must be applied.

3.17.2. Relationship

(1) A customer that exhibits one or more of the following characteristics:

(a) the customer's source of wealth and/or source of funds cannot be easily verified or where the audit trail has been deliberately broken and/or unnecessarily layered;
(b) the customer's affairs are structured in a complex manner, making it easier to conceal underlying beneficial owners and beneficiaries;
(c) the customer's structure has no apparent legitimate economic purpose or rationale;
(d) the customer requests the adoption of undue levels of secrecy within a relationship and/or transaction;
(e) the customer has been the subject of a SAR;
(f) the customer requests products or services in one country or territory when there are very similar products or services in his home country or territory and where there is no legitimate economic or other rationale for requiring the product or service abroad;
(g) the customer makes or holds high value balances or investments which are disproportionately large to that particular customer, product or service set;
(h) the customer uses companies which have, or have the power to, issue bearer shares or other bearer instruments; or
(i) the customer has inappropriately delegated authority.

3.17.3. Connection to Industry

(1) A customer with a connection to one or more of the following:

(a) arms trading;
(b) gambling and casinos;
(c) pharmaceuticals;
(d) charities and NPOs with substantial operations in high-risk jurisdictions;
(e) construction and infrastructure (in particular projects funded by government);
(f) development and other types of overseas assistance;
(g) mining and natural resource extraction;
(h) the provision of public goods and/or utilities;
(i) dealing in precious metals and precious stones, or other luxurious goods;
(j) dealing in luxury vehicles (such as sports cars, ships, helicopters and planes);
(k) dealing in high-end real estate; or
(l) other cash intensive businesses.

3.17.4. Product, Service or Delivery Channel

(1) A customer provided with one or more of the following by the firm:

(a) private banking services;
(b) cash or pseudonymous (i.e. crypto-currency) transactions;
(c) the establishment of legal persons or legal arrangements to act as personal asset-holding vehicles;
(d) hold mail or retained mail arrangements; or
(e) safe custody arrangements, e.g. custody of physical assets or chattels.

3.18. Lower Risk Indicators

(1) The following is a non-exhaustive list of lower risk indicators for customers which the firm may consider when preparing a profile:

(a) a business subject to, and which effectively implements, the requirements to combat ML and FT as set out within the FATF Recommendations and which is effectively supervised or monitored to ensure compliance with those FATF Recommendations;
(b) a public 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;
(c) a public administration or enterprise;
(d) a customer whose funds are part of a pooled client money account held in the name of an Appendix C business;
(e) a natural person who is actively employed with a regular source of income which is consistent with the employment being undertaken;
(f) a Bailiwick resident natural person, or legal person owned by a Bailiwick resident, with a business relationship which is understood by the firm;
(g) a customer represented by those whose appointment is subject to court approval or ratification, e.g. an executor or liquidator;
(h) a product or service where the provider does not permit investment or payment other than from the customer or repayment other than to the customer;
(i) a retirement scheme (which for the avoidance of doubt includes pension, superannuation or similar schemes that provide retirement/savings benefits to employees) where contributions are made by way of deduction from wages or from the sponsoring company's revenues and where the scheme rules do not permit the assignment of a member's interest under the scheme;
(j) a life insurance policy where the annual premium is no more than €1,000 or a single premium of no more than €2,500;
(k) an insurance policy for a pension scheme where there is no surrender clause and the policy cannot be used for collateral;
(l) a customer based in a country or territory identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML and CFT systems; or
(m) a customer based in a country or territory identified by credible sources as having a low level of corruption or other criminal activity.

(2) The existence of one of the above characteristics must not automatically lead to an overall low-risk rating. The above risk factors must be considered in conjunction with any other risk factors identified in respect of the customer, both singularly and in combination, prior to determining an overall risk rating.

Chapter 4
Customer Due Diligence

Contents of this Chapter

Schedule 3 Requirements

The requirements of Schedule 3 to the Law to which the Commission Rules and guidance in this chapter relate are:

- Paragraph 3, which provides for a specified business to identify and assess the risks of ML and FT, both in respect of its business as a whole and its individual business relationships or occasional transactions. Schedule 3 also provides for a firm to ensure that its policies, procedures and controls are effective and appropriate to the assessed risk.

  Paragraph 3 Hyperlink

- Paragraph 4, which provides for the required CDD measures, when and to whom they should be applied.

  Paragraph 4 Hyperlink

- Paragraph 7, which provides for the timing of identification and verification of identity.

  Paragraph 7 Hyperlink

- Paragraph 8, which makes provisions in relation to anonymous accounts and shell banks.

  Paragraph 8 Hyperlink

- Paragraph 9, which provides for non-compliance with CDD measures.

  Paragraph 9 Hyperlink

- Paragraph 10, which provides for the CDD measures to be undertaken in introduced business relationships.

  Paragraph 10 Hyperlink

- Paragraph 15, which makes provisions in relation to corporate governance and the review of compliance, including the requirement to appoint an FCCO.

  Paragraph 15 Hyperlink

4.1. Introduction

(1) This chapter sets out the Commission Rules and provides guidance in respect of CDD, including details of the policies, procedures and controls required by the firm in order to meet the CDD requirements.

(2) The content of this chapter should be read in conjunction with the following three chapters: Natural Persons; Certification; and Legal Persons and Legal Arrangements. These chapters specify the CDD requirements by type of customer (or beneficial owner or underlying principal) with which the firm is entering into a business relationship or undertaking an occasional transaction.

Chapter 5 – Natural Persons

Chapter 6 – Certification

Chapter 7 – Legal Persons and Legal Arrangements

(3) Reference should also be made to the following chapters which provide details of the ECDD and ACDD obligations, together with the circumstances in which the firm can utilise SCDD and the details of such:

Chapter 8 – Enhanced and Additional Customer Due Diligence

Chapter 9 – Simplified Customer Due Diligence

4.2. Overriding Obligations

(1) In accordance with subparagraph 4(2) of Schedule 3, the firm shall undertake 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 that:
    (i) notwithstanding any exemptions or thresholds pursuant to Schedule 3, any party to a business relationship is engaged in ML and/or FT, or
    (ii) it is carrying out a transaction on behalf of a person, including a beneficial owner or underlying principal, who is engaged in ML and/or FT; and
(d) the firm has doubts about the veracity or adequacy of previously obtained customer identification data.

(2) The firm shall also undertake CDD when carrying out occasional transactions which are wire transfers in the circumstances detailed in the Wire Transfers chapter of this Handbook.

Chapter 14 - Wire Transfers

(3) In accordance with the requirements of subparagraphs 8(1) and 8(2) of Schedule 3, the firm shall ensure that for all customers it does not:

(a) set up or keep anonymous accounts;
(b) set up or keep accounts in fictitious names;
(c) enter into, or continue, a correspondent banking relationship with a shell bank; and
(d) enter into, or continue, a correspondent banking relationship where the respondent bank is known to permit its accounts to be used by shell banks.

4.3. Key Principles

(1) The verification of a customer is an on-going and cumulative process, the extent of which is determined by both the risk attributed to, and the particular circumstances of, the business relationship or occasional transaction.

(2) Verification methods providing evidence of identity and address can come from a range of sources, including physical or digital documents, databases and electronic data sources. These sources may differ in their integrity, suitability, reliability and independence.

(3) The firm should consider the suitability of identification data, including its source and whether underlying probity 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.

(4) Where the firm does not receive, or have sight of, original versions of physical documentation used to verify identity, it must ensure that copy documentation provided to the firm has been certified by a suitable third party.

(5) Further information on the policies, procedures and controls required in respect of certification can be found within chapter 6 of this Handbook.

Certification

(6) Where the firm is not familiar with the form of the identification data obtained to verify identity or address, appropriate measures should be undertaken 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 documentation received.

(7) 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.

(8) 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. In all cases the firm should record its understanding of the document and where relevant the reason why it has not sought to translate the document.

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

(10) Where identification data accepted by the firm to verify identity contains the customer's signature and/or a photograph of the customer, the firm should ensure that the photograph and/or signature is plainly legible on the copy or scan of the document retained by the firm.

4.4. Policies, Procedures and Controls

(1) The firm must have customer take-on policies, procedures and controls in place which provide scope to identify and verify identity to a depth appropriate to the characteristics and assessed risk of the business relationship or occasional transaction.

(2) The firm must judge how much identification and verification information to ask for, what to verify, and how to verify, in order to be satisfied as to the identity of a customer, beneficial owner or underlying principal.

(3) Sound CDD procedures are vital for all firms 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, financial crime and FT;
(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 or FT.

(4) The policies, procedures and controls must:

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

4.5. CDD Utilities

(1) As part of the drive of firms to streamline compliance resources, a number of first and third-party products and services have emerged which leverage digital technologies in order to achieve compliance with one or more of the various strands of AML and CFT obligations. The area where technology is having the greatest impact is in the gathering of CDD for customers, and any beneficial owners and underlying principals.

(2) In light of this technology drive, a number of products and services are available which provide various approaches to customer on-boarding, including identifying and verifying the customer, and beneficial owner and underlying principal, understanding the customer and the nature and purpose of the business relationship or occasional transaction.

(3) While the majority of these products and services simply provide for a more efficient, technology based solution to the more traditional or paper-based processes, there are some which introduce new concepts for conducting CDD, the biggest of which is the emergence of the CDD utility.

(4) The purpose of this section is to provide an overview of the concept of a CDD utility and the expectations of the Commission where the firm utilises such a service. The use of electronic methods or systems for the verification of a natural person are not covered within this section and are considered separately (see section 5.6. of this Handbook); however a CDD utility may utilise electronic verification for natural persons as part of its wider processes.

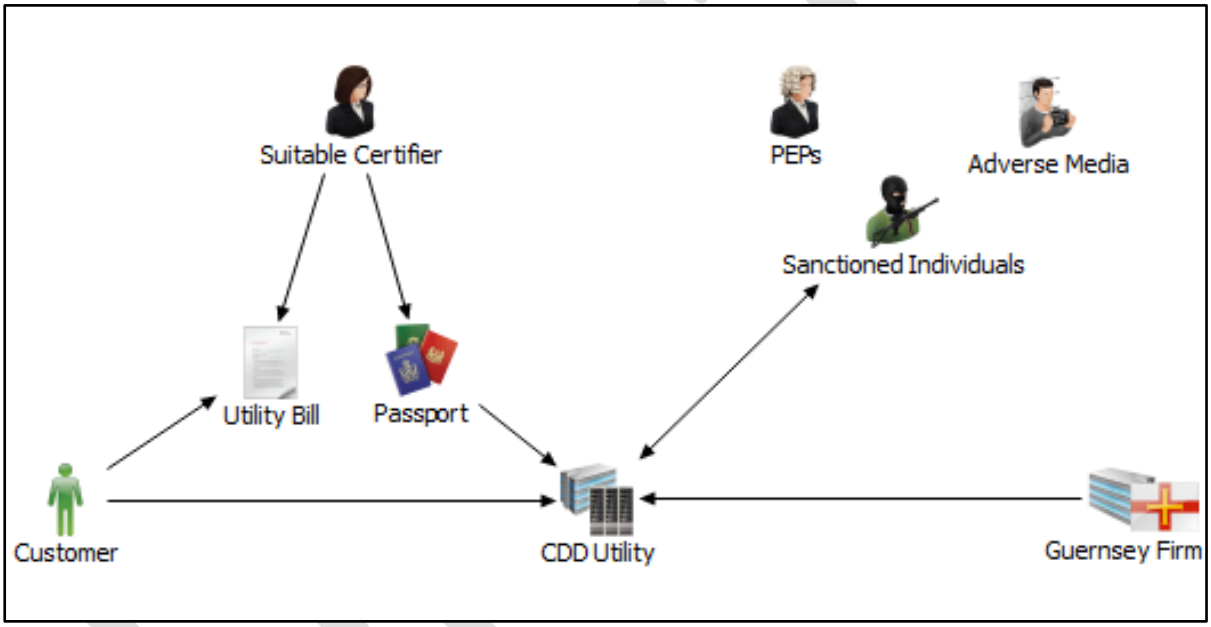
Electronic Verification

(5) Section 3.11. of this Handbook sets-out the requirements for the firm where it wishes to utilise a new technology within its compliance processes. This includes the undertaking of an assessment of the ML and FT risks and vulnerabilities arising from the technology's use prior to its adoption by the board of the firm.

Business Risk Assessment – New Technologies

(6) In addition to the risk assessment obligations set out above, a key requirement for the firm prior to using a CDD utility is to understand the procedures utilised by the system. Part of this understanding is establishing the process by which identification data is received by the utility and the controls utilised to ensure the validity and veracity of the CDD received by the firm.

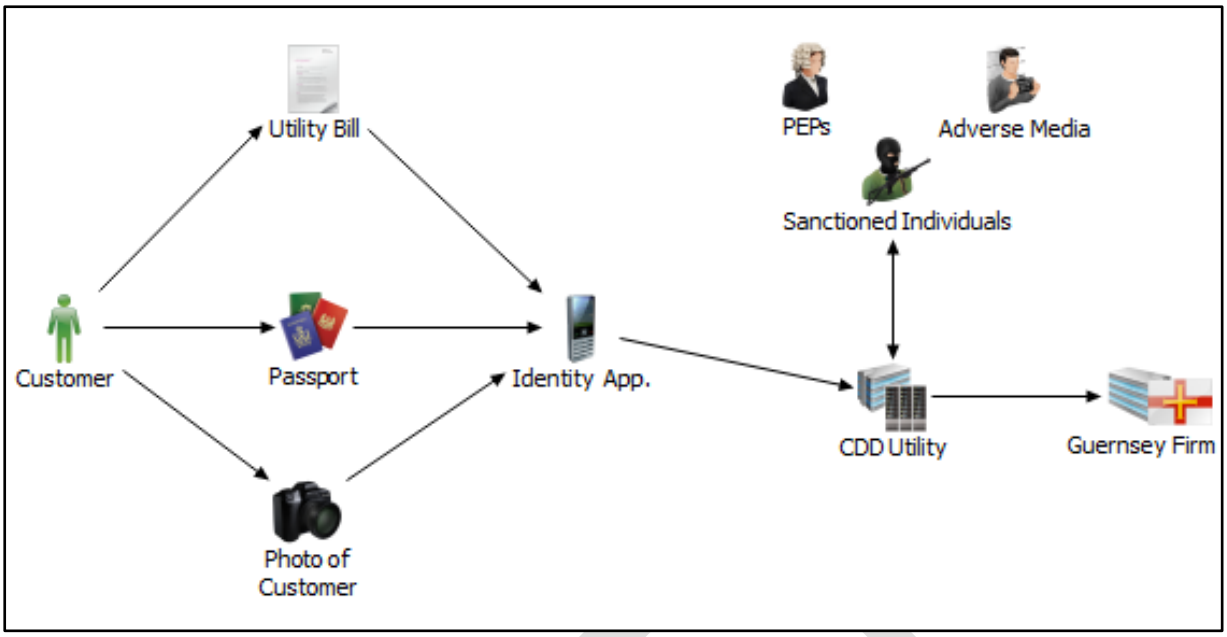
(7) Two examples of CDD utilities are included below and reflect that the obligations of the firm vary depending on the processes used by the utility, e.g. if the firm is establishing a formal outsourcing arrangement with the CDD utility, or if the firm is placing reliance on the CDD utility to gather due diligence on the customer (and any beneficial owner and underlying principal).



(8) In the first example the customer creates an account with the CDD utility and provides information about his identity. The customer uploads copies of his identity and address verification documentation and the physical copies of these documents are provided to a suitable certifier who independently confirms to the CDD utility that he has met the individual and seen the documents in question.

(9) Following completion of the on-boarding process, the identity information and digitally certified identification data of the customer are then stored within the CDD utility under the ownership of the customer. The firm has real-time access to the CDD utility and can review the CDD information about each of its customers.

(10) In the second example the CDD utility includes a front-end application or other method by which the customer can provide his CDD directly to the CDD utility without the need to use a suitable certifier. The requirements for electronic verification and the controls required within such systems are set-out within section 5.6. of this Handbook.



(11) In this example the CDD utility holds a digitally certified package of CDD gathered directly from the customer. This CDD package can then be provided to any number of underlying firms, each of whom can independently verify the digital certification to validate the authenticity of the CDD.

(12) The CDD utility may also undertake ancillary services in relation to the customers within the system, e.g. ongoing sanctions, PEP and/or adverse media screening. Where this is the case, the firm should take measures to establish the accuracy of the screening undertaken and the process by which the firm is advised where a match against one of its customers is identified.

(13) Where the firm wishes to use the services of a CDD utility, whether structured similar to the examples provided previously or not, the firm must give consideration to the risk factors set out in section 3.11.1. of this Handbook, together with the following CDD utility-specific points, before deciding whether to use such a service:

(a) the level of reliance, if any, being placed on the CDD utility by the firm, to have identified and verified the identity of the customer, or any beneficial owner or underlying principal of a customer (see chapter 10 of this Handbook);
(b) whether the firm is establishing a formal outsourcing arrangement with the CDD utility for the purposes of any processes contributing to the firm's compliance with one or more aspect of Schedule 3 or this Handbook;
(c) the ownership of the data held within the utility and the process by which the firm is updated by the customer or the utility where the circumstances of a customer change, e.g. the customer's residential address.

(14) With regard to Rule 4.5.13(a) above, the firm must not place reliance on a CDD utility where it is in turn relying on copy documentation received from another entity (see sections 6.7. and 10.7. of this Handbook).

(15) When utilising the services of a CDD utility, the firm should consider how its record keeping obligations under Schedule 3 and chapter 16 of this Handbook will be met. This is important so as to enable the firm to meet its record keeping obligations, e.g. being able to provide CDD to the FIS upon request, particularly in the event of the firm's relationship with the CDD utility being terminated.

4.6. Timing

(1) In accordance with paragraph 7 of Schedule 3, the identification and verification of a customer shall be carried out before or during the course of establishing a business relationship or before carrying out an occasional transaction.

(2) It is accepted that circumstances may be such that the verification of a customer, or any beneficial owner or underlying principal, cannot commence or be completed until such time as a business relationship has been established, provided the firm has no suspicion as to the reasons causing the delay.

(3) However Schedule 3 does not permit the retrospective identification of a customer, or any beneficial owner or underlying principal, after the establishment of a business relationship or the carrying out of an occasional transaction.

(4) Where the verification of the identity of a customer, or any beneficial owner or underlying principal, 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 the relationship is not high risk;
- (b) obtaining senior management approval to establish the relationship and for any subsequent activity until verification is complete;
- (c) monitoring by senior management of these business relationships to ensure verification of identity is completed as soon as reasonably practicable;
- (d) ensuring funds received are not passed to third parties; and
- (e) establishing limits to the number, type and/or amount of transactions that can be undertaken prior to completion of verification.

(5) The firm should be aware that there may be occasions where the circumstances are such that the business relationship has been established or the occasional transaction has been carried out and the identification and verification procedures cannot be completed. In these circumstances the firm should refer to section 4.9.

Failure to Complete Customer Due Diligence

(6) With regard to occasional transactions, if the identity of the customer is known, verification of identity is not required in the case of occasional transactions (whether single or linked) below the threshold in the 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.

4.7. Collective Investment Schemes

4.7.1. Responsibility for Investor CDD

(1) As part of the process of applying for the authorisation or registration of a closed or open-ended CIS, the board of the CIS (or GP of a LP; trustee of a unit trust; or foundation official of a foundation) must nominate a firm which is licensed under the POI Law and contracted to, or connected with, the CIS to be responsible for meeting the requirements of Schedule 3 and this Handbook for all investors, in addition to its own obligations.

(2) Where nominated, the 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 CIS being authorised or registered.

(3) Where nominated, the 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, e.g. conducting customer risk assessments and identifying, and taking reasonable measures to verify the identity of, any beneficial owner or underlying principal of each investor.

(4) While the activity of gathering CDD (including ACDD and ECDD as necessary) may be undertaken by another party, e.g. under an outsourcing arrangement, the nominated firm will be responsible for ensuring that appropriate CDD is held on all investors which meets the relevant requirements of Schedule 3 and the Commission Rules.

(5) Where the shares of a CIS for which the firm has been nominated are traded on a stock exchange, the nominated firm should refer to the provisions of section 4.7.3. of this Handbook:

Collective Investment Scheme Traded on a Stock Exchange

(6) Where the firm provides services to a CIS and has not been nominated under paragraph 4.7.1.(1), 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.

Collective Investment Schemes Authorised or Registered by the Commission

(7) There may be occasions where the nominated firm will change throughout the life of a CIS, e.g. as a result of a change of designated manager. Where the firm becomes nominated for a CIS which has already been authorised or registered by the Commission, it must advise the Commission in writing as soon as reasonably practicable that it has been so nominated.

4.7.2. Identifying and Verifying Investors in Collective Investment Schemes

(1) This section applies to those firms nominated under paragraph 4.7.1.(1) of this Handbook or acting in the capacity of the administrator or transfer agent of a NGCIS and details the obligations for the collection of CDD for investors, including the beneficial owners and underlying principals thereof.

(2) Fundamental to understanding the CDD obligations for CIS investors is a recognition that the overall arrangements by which interests in the CIS are offered to investors and the overall arrangements under which a CIS consequently deals with investors will fall into one of two broad categories: direct investments and indirect investments.

(3) It should be noted that one CIS may have both categories of relationships and the relationship used in any particular case depends on a variety of characteristics, including the nature of the CIS, the types of investors and the jurisdiction in which the CIS's shares are issued or distributed.

4.7.2.1. Direct Investments

(1) In the case of a direct investment, the investor will ultimately be investing in their personal capacity, i.e. in their own name or through a personal asset vehicle. By virtue of being nominated under paragraph 4.7.1.(1), the firm is likely to have a direct relationship with that investor and may receive/process the investor's application.

(2) When dealing with a direct investment, the firm must treat the investor as if it were its customer and identify and verify the identity of the investor, including identifying, and taking reasonable measures to verify the identity of, the beneficial owner and any underlying principal, in accordance with the identification and verification requirements of Schedule 3 and this Handbook for natural persons, legal persons and legal arrangements.

Natural Persons
Legal Persons and Legal Arrangements

4.7.2.2. Indirect Investments

(1) There may be occasions where the firm does not have a direct relationship with an underlying investor and interests in the CIS are instead distributed by or through FSBs such as banks, broker-dealers, insurance companies/agents, investment advisors, financial planners, regulated platforms, or other financial institutions.

(2) In such circumstances shares may be held by or through an FSB in multi-client pooled/omnibus-type accounts or other arrangements used to collect together funds from a variety of sources for onward investment under the direct control of the FSB (collectively referred to as an "omnibus account").

(3) Omnibus accounts are used when an FSB acquires the shares in a CIS on behalf of its customers, i.e. the ultimate underlying investors. In such cases the shares are usually acquired in the name of the FSB; however there may be cases where that business establishes an account with the CIS which specifies sub-accounts on behalf of named investors.

(4) This sub-section relates to, and sets out the Commission Rules and guidance in respect of, an investment made into an authorised or registered CIS by an Appendix C business (or a wholly owned subsidiary thereof resident or domiciled in a country or territory listed in Appendix C which applies the AML/CFT policies, procedures and controls of its parent entity), where there is an indication or assumption that the Appendix C business is transacting on behalf of an underlying investor rather than transacting on its own behalf. For the purposes of this sub-section these entities will be collectively referred to as 'Appendix C businesses'.

(5) 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 omnibus account being used to mask the true beneficial ownership of investments into Guernsey-based CISs, particularly where the omnibus account has a very limited number of underlying investors.

(6) Where an Appendix C business is investing in a CIS on behalf of one or more underlying investors via an omnibus account, the firm may utilise the measures set out in Rule 4.7.2.2.(8), provided that the criteria in Rule 4.7.2.2.(7) are met.

(7) In order to treat the Appendix C business as its customer in accordance with paragraph 4.7.2.2.(4), the firm must ensure that the following criteria are met:

(a) the customer is an Appendix C business operating an omnibus account;
(b) the firm understands the purpose and intended nature of the business relationship and is satisfied that there is a legitimate business reason for the use of the Appendix C business and the omnibus account; and
(c) the ML and FT risks of the business relationship with the Appendix C business have been assessed as low and the firm is satisfied that any risks specifically arising from the use of the omnibus account have been appropriately mitigated.

(8) Based upon its risk assessment of the business relationship and where the conditions in Rule 4.7.2.2.(7) are met, the firm can exercise its own judgement in the circumstances as to the level of CDD to be applied. As a minimum the firm must:

(a) identify and verify the identity of the Appendix C business in accordance with the requirements of chapter 9 of this Handbook;
(b) receive written confirmation from the Appendix C business (and be satisfied as to the content and veracity of such confirmation) which:
  (i) confirms that the Appendix C business has appropriate risk-grading procedures in place to differentiate between the CDD requirements for high and low risk relationships;
  (ii) contains adequate assurance that the Appendix C business conducts appropriate and effective CDD procedures in respect of its customers, including ECDD measures for PEPs and other high risk relationships;
  (iii) confirms that the account will only be operated by the Appendix C business and that the Appendix C business has ultimate effective control over the product or service; and
  (iv) confirms that the Appendix C business will provide upon request identity information (in accordance with chapters 5 and 7 of this Handbook) on their customers who are ultimately invested in the CIS; and
(c) identify any natural persons who ultimately controls CIS through ownership or other means.

Simplified Customer Due Diligence – Appendix C Business

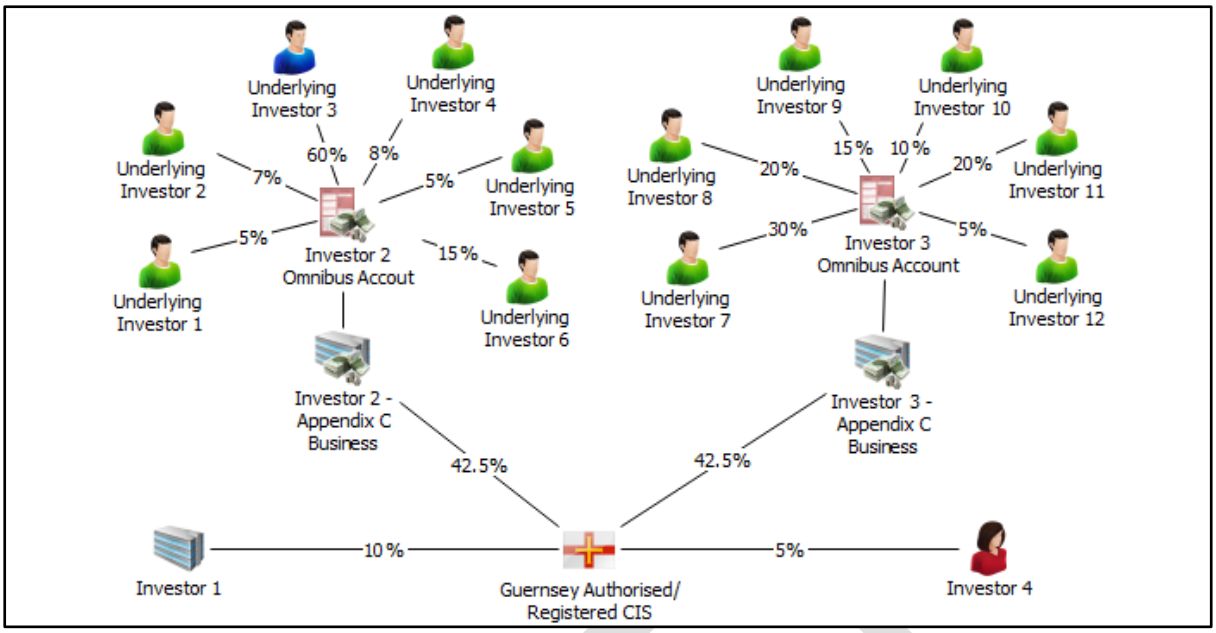
(9) For the purposes of Rule 4.7.2.2.(8)(c), the requirement to identify underlying investors applies to those underlying investors ultimately controlling the CIS through ownership or other means, rather than in the Appendix C business' holding in the CIS. The firm should take reasonable measures to determine whether an underlying investor ultimately controls the CIS through ownership or other means.

(10) When determining what constitutes control through ownership in a CIS, reference should be made to section 7.4.2. of this Handbook, or the equivalent section depending on the type of legal person or legal arrangement used for the CIS.

Understanding the Beneficial Ownership of Legal Persons

(11) Determining whether a natural person ultimately controls a CIS through ownership or other means could be achieved by requiring the Appendix C business to provide, as part of its written confirmations in accordance with Rule 4.7.2.2.(8)(b), the identity of any underlying investors ultimately holding more than a specified percentage of the Appendix C business' holding, calculated by the firm to amount to a controlling interest in the overall capital of the CIS.

(12) In the case of the example overleaf, the firm has determined that, based on the CIS being a Guernsey legal person, a 25% holding in the CIS constitutes a controlling interest. As such, based on their percentage holdings, any natural person who holds ≈59% of either omnibus account would have to be identified in accordance with Rule 4.7.2.2.(8)(c). In this example there is one underlying investor, in blue, who holds a controlling interest. The firm would therefore be required to comply with the requirements of Rule 4.7.2.2.(16) below for this individual.



(13) Where the firm has utilised the provisions of Rule 4.7.2.2.(8), the firm must prepare and retain documentary evidence of the following:

(a) the adequacy of its process to determine the risk of the business relationship with the Appendix C business and the reasonableness of its conclusions that it is a low risk relationship;
(b) that it has undertaken CDD procedures in respect of the Appendix C business; and
(c) that the relationship relates solely to the Appendix C business' provision of an omnibus account for the purposes of investment into the relevant CIS.

(14) The firm should always consider whether the risks would be better managed if the firm undertook CDD on an underlying investor, including any beneficial owner or underlying principal, for which the Appendix C business is acting rather than treating the Appendix C business as the customer.

(15) Where the firm determines that it cannot apply the measures in Rule 4.7.2.2.(8), e.g. because the investor is not an Appendix C business or the risk of the business relationship has been assessed as being other than low, the firm must treat the underlying investors as if they were direct investments and perform its own CDD measures as follows:

(a) open individual accounts in the name of each underlying investor and conduct CDD on each of those underlying investors, including the beneficial owners and underlying principals; or
(b) open an omnibus account in the name of the Appendix C or other business, provided that the firm also receives a complete list of the underlying investors from the Appendix C business to allow it to perform its own CDD measures on those investors.

(16) When identifying, and taking reasonable measures to verify, the identity of underlying investors, including the beneficial owner and any underlying principal, 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.

Natural Persons
Legal Persons and Legal Arrangements

4.7.3. Collective Investment Scheme Traded on a Stock Exchange

(1) There are fundamental differences between authorised and registered open-ended and closed-ended CISs technically listed on a stock exchange and closed-ended CISs ("CECISs") that are traded on a stock exchange.

(2) Traded CECISs do not operate in the same manner as listed CISs. Other than during an offer period, e.g. an initial public offering, traded CECISs do not directly open accounts for investors, while listed CISs will.

(3) The shares of a traded CECIS 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, traded CECISs 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, while listed CISs do.

(4) These fundamental differences are 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'.

(5) Where the shares of a CECIS are traded on a stock exchange prescribed by the [TBC] Regulations, in accordance with paragraph 4(5) of Schedule 3 it is not necessary for the firm nominated by that CECIS under paragraph 4.7.1.(1) to identify and verify the identity of investors in that scheme.

[TBC] Regulations

(6) Notwithstanding the above, the remaining obligations within Schedule 3 and this Handbook in respect of a CECIS apply, including the requirement to file disclosures where suspicious activity is suspected or identified. The Commission's expectations of the nominated firm are set out in the paragraphs that follow.

(7) For authorised and registered open-ended and closed-ended CISs technically listed on a stock exchange, the firm should follow the requirements for identifying and verifying investors in accordance with section 4.7.2. of this Handbook.

Identifying and Verifying Investors in Collective Investment Schemes

4.7.3.1. Primary Market

(1) Where the firm has been nominated under paragraph 4.7.1.(1), at the time of the initial offering it must make sure that it understands all routes that investors could subscribe into the authorised or registered CECIS and the likely business relationships which will be established.

(2) The nominated firm must then undertake customer risk assessments and gather CDD (including ACDD and ECDD as applicable) for each placing agent, broker/dealer and other market intermediary, together with any direct investor relationships in relation to any open offer for subscription in accordance with Rule 4.7.2.1.(2).

4.7.3.2. Secondary Market

(1) After the initial offering is completed, an investor will generally purchase or sell shares through their broker/dealer or market intermediary which will execute a transaction on the stock exchange and not with the traded CECIS or nominated firm. As a consequence, following the initial offering the nominated firm will not enter into any new business relationships with investors.

(2) The nominated firm is therefore not required to conduct CDD on any underlying investors in a traded CECIS. The responsibility for CDD is placed upon the established broker/dealer or market intermediary to a transaction.

(3) The firm must therefore treat a traded CECIS like any other legal person whose shares are listed on a stock exchange in accordance with subparagraph 4(5) of Schedule 3.

(4) Notwithstanding the above, there may be occasions when an investor buys or sells shares directly with an authorised or registered CECIS in an off-market transaction. In such a scenario the nominated firm must treat the investor as if it were its customer, including identifying, and taking reasonable measures to verify the identity of, the beneficial owner and any underlying principal, in accordance with the identification and verification requirements of Schedule 3 and this Handbook for natural persons, legal persons and legal arrangements.

Natural Persons
Identification and Verification of Legal Persons

4.8. Acquisition of a Business or Block of Customers

(1) There are circumstances where the firm may acquire another specified business with established business relationships or a block of customers, e.g. by way of asset purchase from another specified business or from a non-Bailiwick firm.

(2) 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.

(3) 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 Rule 2.7.(1).

(4) In addition to conducting due diligence on the vendor, the firm may consider it appropriate to rely on the information and documentation 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 for each customer acquired.

4.9. Failure to Complete Customer Due Diligence

(1) Where the firm has been unable, within a reasonable time frame, to complete CDD procedures in accordance with the requirements of Schedule 3 and this Handbook, it must assess the circumstances and ensure that appropriate action is undertaken as required by paragraph 9 of Schedule 3.

(2) 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, e.g. 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.

(3) Where the firm has lost contact with a customer and the termination of a business relationship cannot be completed, 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.

(4) 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 relationship can be terminated and any associated funds returned to the customer.

(5) 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 this is not possible, for instance because the originating bank account has been closed, funds must be paid to an account in the name of the customer.

(6) Where the firm has terminated, or not proceeded with establishing, a business relationship or occasional transaction, it must give consideration to the circumstances giving rise to the failure to complete CDD and whether these warrant a disclosure to the FIS.

Chapter 5
Natural Persons

Contents of this Chapter

Schedule 3 Requirements

The requirements of Schedule 3 to the Law to which the Commission Rules and guidance in this chapter particularly relate are:

- Paragraph 3, which provides for a specified business to identify and assess the risks of ML and FT, both in respect of its business as a whole and its individual business relationships or occasional transactions. Schedule 3 also provides for a firm to ensure that its policies, procedures and controls are effective and appropriate to the assessed risk.

  Paragraph 3 Hyperlink

- Paragraph 4, which provides for the required CDD measures, when and to whom they should be applied.

  Paragraph 4 Hyperlink

- Paragraph 5, which provides for ACDD and ECDD measures in respect of business relationships and occasional transactions where the circumstances necessitate additional measures or the business relationship or occasional transaction has been assessed as high risk.

  Paragraph 5 Hyperlink

- Paragraph 6, which provides for SCDD measures to be applied to business relationships which have been identified as being low risk relationships.

  Paragraph 6 Hyperlink

- Paragraph 15, which makes provisions in relation to corporate governance and the review of compliance, including the requirement to appoint an FCCO.

  Paragraph 15 Hyperlink

5.1. Introduction

(1) Establishing that any customer, beneficial owner or underlying principal is the person that he/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 underlying principal, is that person – by verifying from identification data, satisfactory confirmatory evidence of that person's identity.

(2) This chapter sets out the aspects of a natural person's identity which must be established together with the identification data to be gathered to verify the identity of that natural person. These requirements apply when entering into a business relationship or conducting an occasional transaction with a natural person, or for any natural person who is the beneficial owner or underlying principal of a customer which is a legal person or legal arrangement.

(3) In accordance with Schedule 3, a natural person acting in one or more of the following capacities must be identified and his identity verified using identification data:

(a) the customer;
(b) a beneficial owner or controller of the customer;
(c) an underlying principal of the customer;
(d) a person who is a third party on behalf of whom the customer is purporting to act; or
(e) a person purporting to act on behalf of the customer (e.g. a natural person with signing authority over an account, or with a power of attorney in respect of the customer's affairs), and his authority to so act shall also be verified.

5.2. Establishing the Identity of a Natural Person

(1) Where the firm is required to identify a natural person who is the customer (or beneficial owner or underlying principal) it must collect relevant information on identity which includes:

For all customers:

(a) legal name;
(b) any former names (such as maiden name) and any other names used;
(c) principal residential address; and
(d) date of birth.

For customers other than low risk, additionally:

(e) place of birth;
(f) nationality (including all nationalities where the individual holds more than one); and
(g) a government issued personal identification number or other government issued unique identifier.

(2) In accordance with paragraph 4 of Schedule 3, when identifying a natural person the firm shall make a determination as to whether the natural person is, or has been, a PEP or entrusted with a prominent function by an international organisation. If the natural person is a PEP, the firm must also determine whether he/she is a foreign PEP or a domestic PEP. Further information can be found in chapter 8 of this Handbook.

Enhanced and Additional Due Diligence - Politically Exposed Persons

(3) Where the firm has determined that a business relationship or occasional transaction is high risk, in accordance with paragraph 5 of Schedule 3 the firm shall apply ECDD which includes taking one or more additional steps to develop a greater understanding of the customer and the business relationship or occasional transaction. This could include obtaining further identification data for a natural person who is the customer (or any beneficial owner or underlying principal) as would be appropriate in the circumstances, such as:

(a) the customer's occupation;
(b) the extent of the customer's assets; and
(c) publicly available information about the customer.

5.3. Verifying the Identity of a Natural Person

(1) The firm must verify the natural person's identity using identification data, the extent of which is to be determined on the basis of the risk rating attributed to the relationship. As a minimum the firm must verify:

For all customers:

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

For standard risk customers, additionally:

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

For high risk customers, additionally:

(f) a government issued personal identification number or other government issued unique identifier.

(2) In order to verify the above and other data collected, the following identification data is considered to be the best possible:

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

(3) 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 identity of the natural person.

(4) When changes occur which result in changes to a natural person's profile, e.g. 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.

5.4. Verification of Residential Address

(1) The following are considered to be suitable 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 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.

(2) 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 Customers

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

(2) Where the firm has determined that an individual has a valid reason for being unable to produce more usual documentation to verify residential address and who would otherwise be excluded from establishing a business relationship or undertaking an occasional transaction with the firm, satisfactory verification of address may be established by other means, e.g.:

(a) a letter from a director or officer of a reputable overseas employer that confirms residence at a stated overseas address (or provides detailed directions to locate a place of residence); or
(b) any of the means provided in section 5.4. without regard to any restrictions imposed on such documents.

5.5. Online Bank Statements or Utility Bills

(1) Where the 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 address verification which has been delivered to the customer by post. However, the receipt of such items via the traditional postal system is becoming more limited following a rise in the use of online billing or the delivery of bank or utility statements via e-mail ("an electronic statement").

(2) Examples of electronic statements include:

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

(3) Where the firm wishes to accept an electronic statement as verification of address, it must undertake one of the following steps and document the result of the action taken:

(a) make a telephone call to the customer via a landline telephone number that has been independently verified as belonging to the address in question;
(b) corroborate the address of the natural person using independent commercial or electronic data sources, e.g. a land registry, electoral roll or similar; or
(c) have a representative of the firm present with the customer while they log onto the website of the bank/credit card or utility provider and watch while they request or download an electronic statement and witness the receipt or downloading of the electronic statement.

5.6. Electronic Verification

(1) 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.

(2) Electronic verification can be used to verify all or any combination of the mandatory verification requirements. Where electronic verification does not fulfil all of these requirements, the firm must use other methods to meet the requirements of Rule 5.3.(1). of this Handbook.

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

(4) Whilst the use of electronic verification can help to reduce the time and cost involved in gathering information and documentation on a natural person, the firm should be mindful of any additional risks posed by placing reliance on an electronic method or system, e.g. understanding the method and level of review and corroboration, and the potential for the system to be abused. These risks should be considered as part of the firm's technology risk assessment.

Business Risk Assessment – New Technologies

(5) Knowledge and understanding of the functionality and capabilities of the 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 confirmation source to match data enhances the assurance of authenticity.

5.7. Independent Data Sources

(1) 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, e.g. 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.

(2) 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.

(3) Where an independent data source does not provide for the verification of all of the data points required by Rule 5.3.(1), 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.

(4) When relying on independent data sources to verify identity, the firm should ensure that the source, scope and quality of that data are suitable and sufficient and that the process provides for the information to be captured and recorded, e.g. where the firm utilises the services of a credit reference agency to identify natural persons, the reliance placed on a verification report with only corroborative checks should naturally be less than a report for a natural person with multiple primary checks.

5.8. Guarding Against the Financial Exclusion of Bailiwick Residents

(1) There may be occasions when a natural person encounters difficulties in providing evidence of his Bailiwick residential address using the sources identified earlier in this chapter. Examples of such circumstances include:

(a) a seasonal worker 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 (e.g. 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.

(2) Where a natural person has a valid reason for being unable to produce the requested documentation and who would otherwise be excluded from accessing the firm's products and services, identification procedures should provide for alternative means of verifying a natural person's Bailiwick residential address. The following are examples of alternative 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 seasonal worker, the worker's residential address in his 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
Certification

Contents of this Chapter

6.1. Introduction

(1) Certification is the process whereby, in lieu of a customer presenting himself and his identification data in person to the firm, the customer instead uses a suitable trusted third party to confirm a positive link between his identity and his identification data. The certified identification data is then provided to the firm as verification of the customer's identity.

(2) The use of third party certification serves to mitigate the risk arising from a business relationship or occasional transaction within which the firm has no face-to-face contact with the customer, beneficial owner or underlying principal and 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) At its core, the two-fold purpose of certification is to provide assurance to the firm that the natural person who is their customer (or a beneficial owner or underlying principal of a customer) is who he purports to be and is the owner of the identification data used for the purpose of the firm verifying identity.

(4) While traditional certification has involved the use of a natural person of sufficient standing and subject to appropriate ongoing requirements in respect of his integrity, it should be noted that the trusted third party could take the form of an electronic means of validation.

(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 electronically certifying scanned identification data; and
(c) electronic methods of certifying identification data.

6.2. Obligations

(1) For certification to be effective, the certifier that the firm is relying on should be a trusted third party providing assurance that the identification data verifying aspects of the customer's identity (or that of a beneficial owner or underlying principal) is a true copy of an original document (or extract thereof).

(2) 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 documents;
(b) a policy in relation to those categories of 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 documents on which the firm intends to rely.

(3) The firm must exercise caution when accepting certified copy 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

(1) 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 to confirm the following:

(a) that he has seen the original identification data verifying identity or residential address; and
(b) adequate information about himself 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.

(2) For the purposes of Rule 6.3.(1)(b) 'adequate information' should be provided by the certifier either on the certified document or attached to that document by way of a covering letter or other record which accompanies the certified document and 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 (e.g. postal address; contact telephone number; and/or e-mail address).

(3) Certification by a natural person can take two forms. Firstly, where the certification is stamped or written onto a photocopy of an identification document or attached thereto. Secondly, electronic certification where paper-based documentation is scanned and validated electronically.

(4) The process for utilising electronic certification mirrors that set out for paper-based documentation. Should the certifier accept the documentation presented by the customer, then using digital encryption or a suitably robust alternative, the certifier will apply a digital signature (or equivalent) to an electronic copy of the physical document.

(5) Where the firm utilises a system allowing for natural persons to certify documents electronically, or otherwise receives identification data which has been certified by a natural person electronically, it must satisfy itself of the veracity of the certification process prior to accepting a document certified in such a manner.

6.4. Assessing the Suitability of Natural Person Certifiers

(1) Where copy documents certified by a natural person are accepted, regardless of the manner or form of the documentation, the firm must satisfy itself that the certifier is a suitable and appropriate person to provide validation of the identity documentation based on the assessed risk of the business relationship or occasional transaction, together with the level of reliance being placed on the certified documents.

(2) The firm should, as part of its compliance arrangements, have in place a procedure which explains its assessment process to determine whether an individual is suitable and therefore whether reliance can be placed upon the certified documentation provided. The risk appetite of the firm should inform its policy in this regard and the policy should take account of factors including whether the certifier:

(a) holds an appropriate public position with a high level of trust and for which background checks or similar vetting of his fitness and propriety has occurred;
(b) is a member of a professional body which undertakes independent oversight of compliance with its own rules or standards of professional conduct;

(c) 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;
(d) 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
(e) is subject to other professional rules or a member of an industry body (or equivalent) providing for the integrity of his conduct.

(3) The firm's procedures 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.

(4) As part of the steps taken to validate the credentials of a certifier, the firm may also include the consideration of factors such as: the reputation and track record of the certifier; the firm's previous experience of accepting certified documents from persons in the same profession or country or territory; the adequacy of the framework to counter ML and FT in place in the country or territory in which the certifier is located; and the extent to which the framework applies to the certifier.

6.5. Certification Requirements for Electronic System Certifiers

(1) Through the emergence of the RegTech movement, in addition to the traditional paper-based method of identity verification, the firm can now also utilise electronic means of gathering natural person identification data, details of which are provided in Natural Persons chapter of this Handbook.

Natural Persons – Electronic Verification

(2) As technology has evolved and software enhanced, greater controls have been incorporated into the validation process which have effectively negated the need for natural person certification, allowing for the confirmation of customer identity and the corroboration between the natural person and the verification documents used. Examples of these controls include:

(a) a requirement for photographs to be taken at the time of the system's use (e.g. the application takes control of the device's camera and automatically captures images of the document(s)/natural person);
(b) the inclusion of anti-impersonation measures (e.g. a requirement for the customer to verbally repeat words, phrases or passcodes dictated by the firm during a video call);
(c) the corroboration of the images within an identity document (both physically and/or stored on the RFID chip), together with a self-taken photograph of the customer;
(d) a process whereby the images taken are independently verified, either by a suitably trained individual or computer system, to confirm the authenticity of the documents used to verify identity (e.g. that the documents have not been fraudulently altered, are listed on a missing/stolen documents list, etc.);
(e) the corroboration of biometric information (e.g. finger prints, voice identification, etc.); and/or
(f) geotagging/geolocation (i.e. the inclusion of geographical identification metadata to confirm the location in which the user interacted with the system).

(3) Where the firm adopts a system providing for the electronic verification of customer identity, it must assess the veracity of the controls inherent within the system in order to determine whether the firm can place reliance on the results produced, or if additional steps are necessary to complement the existing controls.

(4) The additional steps undertaken by the firm could include:

(a) requiring a representative of the firm to be present with the customer when the on-boarding software is being used; and/or
(b) issuing each new customer with a code or similar unique identifier which must be included within the photographs taken of the customer and/or identification data.

6.6. Certification of Documentation for Legal Persons and Legal Arrangements

(1) 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 certifier.

(2) 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 certifier.

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

(4) Certification can be provided either through the certifying of a hard-copy document, or through the use of a digital signature applied to an electronic copy of the document.

(5) 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 relationship.

6.7. Copy Certified Documentation

(1) The firm should not place reliance upon copies of previously certified documentation other than for justifiable instances. The firm should always consider the risk of reliance on certified copy documentation and consider whether it would be appropriate to obtain originals.

(2) The firm may only accept certified copy documentation when it can be verified that the current certifier (i.e. the third party certifying the copy documentation provided to the firm) has actually seen the original or originally certified documentation or met the individual in question.

Chapter 7
Legal Persons and Legal Arrangements

Contents of this Chapter

Schedule 3 Requirements

The requirements of Schedule 3 to the Law to which the Commission Rules and guidance in this chapter particularly relate are:

- Paragraph 3, which provides for a specified business to identify and assess the risks of ML and FT, both in respect of its business as a whole and its individual business relationships or occasional transactions. The paragraph also provides for a firm to ensure that its policies, procedures and controls are effective and appropriate to the assessed risk.

  Paragraph 3 Hyperlink

- Paragraph 4, which provides for the required CDD measures, when and to whom they should be applied.

  Paragraph 4 Hyperlink

- Paragraph 5, which provides for ACDD and ECDD measures in respect of business relationships and occasional transactions where the circumstances necessitate additional measures or the business relationship or occasional transaction has been assessed as high risk.

  Paragraph 5 Hyperlink

- Paragraph 6, which provides for SCDD measures to be applied to business relationships which have been identified as being low risk or in accordance with the NRA.

  Paragraph 6 Hyperlink

- Paragraph 10, which provides for the CDD measures to be undertaken in introduced business relationships.

  Paragraph 10 Hyperlink

- Paragraph 15, which makes provisions in relation to corporate governance and the review of compliance, including the requirement to appoint an FCCO.

  Paragraph 15 Hyperlink

7.1. Introduction

(1) The identification and verification requirements in respect of customers who are legal persons or 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 customer also involves a number of natural persons, whether as beneficial owners (or equivalent), directors (or equivalent) or underlying principals, who have the power to direct the movement of a customer's funds or assets.

(2) The purpose of this chapter is to set out the information which the firm must obtain as a minimum for a customer, or beneficial owner or underlying principal of a customer, which is a legal person or legal arrangement.

(3) On the basis of the assessed ML and FT risks of the particular customer/product/service combination, the firm must consider how the identity of the customer and connected persons must be verified and the identification data in respect of those persons which must be obtained, including ACDD and/or ECDD where necessary.

(4) 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.

(5) Legal arrangements do not have separate legal personality and therefore form business relationships through their trustees. It is the trustee of the trust who will enter into a business relationship on behalf of the trust and should be considered, along with the trust, as the firm's customer.

(6) 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.

(7) The firm should be alive to, and take measures to prevent, the misuse of legal persons and legal arrangements for ML and FT. It is imperative that when compiling a relationship risk assessment, the firm considers the breadth of ML and FT 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.

(8) Where the firm administers a legal person established in Guernsey, it should also have regard 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

(1) 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 first 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, become ever more sophisticated, so too do the ways in which a person may structure his or its affairs in order to mask the true beneficial ownership.

(2) When performing CDD measures in relation to customers that are legal persons or legal arrangements, in accordance with Schedule 3 the firm is required to: identify and verify the identity of the customer; understand the nature of its business; and understand its ownership and control structure. These obligations serve primarily to protect the firm, and in turn the reputation of the Bailiwick as a whole, from its products and services being abused for criminal purposes.

(3) The definition of beneficial owner in the context of legal persons must be distinguished from the concepts of legal ownership and control. On one hand, legal ownership means the natural or legal persons 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, e.g. by owning a controlling block of shares.

(4) 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.

(5) In the context of a trust, beneficial ownership includes both the natural persons receiving benefit from the trust, e.g. a beneficiary, class of beneficiaries or any other person who benefits from the trust, as well as underlying principals being the settlor(s), trustee(s), protector(s), enforcer(s) and any other natural person(s) exercising control over that trust.

(6) Paragraph 4(3)(c) of Schedule 3 requires that the firm identify, and take reasonable measures to verify the identity of, the beneficial owner and any underlying principal of a customer and take measures to understand the ownership and control structure of that customer using identification data.

(7) 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 a beneficial owner or underlying principal and to understand the ownership and control of the customer.

(8) 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.

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

(1) The use of nominee shareholders and nominee directors provides 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 identify the true identity of those persons with ultimate ownership and control of a customer.

(2) The firm must ensure that it considers whether a customer, or beneficial owner or underlying principal, which is a legal person could have nominee shareholders and/or nominee directors. The firm must also have procedures which prevent the misuse of nominee shareholders and nominee

directors, including the means to ensure that the firm identifies, and takes 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 structure.

(3) Where the firm identifies that a legal person has nominee shareholders, in accordance with paragraph 5 of Schedule 3 it shall as a minimum apply ACDD measures as set out in chapter 8 of this Handbook, regardless of the risk rating attributed to the business relationship or occasional transaction.

(4) 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, and take reasonable measures to verify the identity of, the natural person(s) who ultimately control the customer.

7.3.1. Nominee Shareholders

(1) 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 on behalf of another on trust. As a consequence the ultimate beneficial ownership remains undisclosed. In this instance the nominee shareholder cannot be considered the beneficial owner.

(2) Nominee shareholders can be used to hide or obscure the beneficial ownership of a legal person customer or corporate underlying principal, e.g. 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.

(3) In determining effective control, the firm should also consider the types of ownership interests and the power of these interests (e.g. the issue of voting shares or non-voting shares).

(4) 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. A similar approach is adopted in a number of other jurisdictions, such as Jersey and the Isle of Man.

7.3.2. Nominee Directors

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

(2) Steps have been taken within the Bailiwick, and by other jurisdictions, to counter the risk of natural or legal persons acting as nominee director; 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.

(3) Further guidance is provided in the Commission's Code of Practice for Company Directors:

Code of Practice – Company Directors

(4) Where the firm has concerns that a person may be acting as a director on behalf of an undisclosed party, it should satisfy itself that the director's credentials for acting are consistent with the legal person's purpose, e.g. the firm should consider if a directorship is consistent with a natural person's occupation, or whether a director holds other unrelated board appointments.

7.4. Legal Persons

(1) Where a legal person is the customer, or the beneficial owner or underlying principal of a customer, the firm must identify and verify the identity of that legal person, 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 status of 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);
(f) the powers that regulate and bind the legal person;
(g) any natural persons, e.g. underlying principals, directors, authorised signatories or equivalent, with ultimate effective control over the capital or assets of the legal person; and
(h) any person purporting to act on behalf of the legal person, including his authority to so act.

(2) In addition to the above, in accordance with paragraph 4(3)(c) of Schedule 3 the firm shall also identify, and take reasonable measures to verify the identity of, the beneficial owner and any underlying principal of the legal person as set out in section 7.4.2. of this Handbook.

Understanding the Beneficial Ownership of Legal Persons

(3) Where the legal person (taking into account any beneficial owner and underlying principal of the legal person) presents a high risk or requires the application of ACDD, the firm should refer to the obligations set out within chapter 8 of this Handbook.

Enhanced and Additional Customer Due Diligence

(4) With regard to the identification and verification of directors (or equivalent) in accordance with Rule 7.4.(1)(g), it may be appropriate to consider directors with effective control as being those who have authority to operate an account or to give the firm instructions concerning the use or transfer of funds or assets. In the case of partnerships; associations; clubs; societies; charities; church bodies; institutes; mutual and friendly societies; and co-operative and provident societies, this 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.

(5) The firm should take a risk-based approach when verifying the authorised signatories of a legal person. Consideration should be given to the level of a signatory's authority and identifying which signatories will provide instructions to the firm and the type of instruction they are authorised to permit.

(6) When verifying the authority of a person to act on behalf of a customer, in addition to verifying the identity of that person, in accordance with paragraph 4(3)(b) of Schedule 3 the firm shall also verify the person's authority to so act.

(7) The CDD measures for customers which are legal persons authorised or registered by the Commission as CISs under the POI Law are set out in section 7.16. of this Handbook.

Collective Investment Schemes Authorised or Registered by the Commission

7.4.1. Verifying the Identity of Legal Persons

(1) One or more of the following examples are considered suitable to verify aspects of the identity of the legal person in accordance with Rule 7.4.(1):

(a) a copy of the Certificate of Incorporation (or equivalent);
(b) a copy of the Memorandum and Articles of Association (or equivalent);
(c) a copy of the latest audited financial statements which show the company name, the identity of the directors and the registered address;
(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 bank account and recording the account signatories; and/or
(j) a personal visit to the principal place of business.

(2) Where the documents obtained are copies of the originals, the firm should refer to the requirements of chapter 6 of this Handbook.

Certification of Documentation for Legal Persons and Legal Arrangements

(3) Where the firm has been unable to verify the identity of the legal person using any of the methods listed on paragraph 7.4.1.(1) above, it must:

(a) document the reasons why the methods set out in paragraph 7.4.1.(1) have not achieved the required level of verification;
(b) document the alternative measures taken to verify the identity of the legal person;
(c) document how the firm considers the steps taken to be sufficient to satisfy the requirements of Schedule 3 and the Commission Rules; and
(d) have approval from the board of the firm to establish or maintain the business relationship or occasional transaction and confirming its satisfaction with the measures taken.

7.4.2. Understanding the Beneficial Ownership of Legal Persons

(1) Paragraph 4(3)(c) of Schedule 3 requires the firm to identify, and take reasonable measures to verify the identity of, the beneficial owner and any underlying principal of a legal person which is the firm's customer and take measures to understand the ownership and control structure of that customer using identification data.

(2) In establishing the beneficial ownership of a legal person, the firm must identify and take reasonable measures to verify (without limitation) the identity of:

(a) any natural person or persons who ultimately control that person through ownership;
(b) any natural person or persons who ultimately control that person through other means; or
(c) any natural person or persons who hold the position of senior managing officials of that legal person.

(3) The measures set out in Rule 7.4.2.(2) above are not alternative options. Establishing the beneficial ownership of a legal person should be considered a cascading process, beginning with 7.4.2.(2)(a) and moving to (b) and ultimately (c) where the previous measure has been applied and has not identified a natural person falling within the definition of beneficial owner.

(4) For the purposes of Rule 7.4.2.(2)(a), in accordance with paragraph 4(8) of Schedule 3 and in turn as defined by regulation 2(1) of the Beneficial Ownership Regulations, a natural person is deemed to control a relevant legal person through ownership if he:

(a) holds, directly or indirectly, more than [TBC]% of the legal person's shares;
(b) holds, directly or indirectly, more than [TBC]% of the voting rights in the legal person; or
(c) holds the right, directly or indirectly, to appoint or remove a majority of the board of directors of the legal person.

(5) It should be borne in mind that a natural person could also indirectly hold an ownership interest in a customer which is a legal person. This situation could arise where the legal person holds the share(s) in question; where the natural person is the beneficial owner of a second legal person which in turn has a majority stake in the relevant legal person; or through other ownership interests, e.g. shareholders' agreements or the holding of convertible stock or any other outstanding debt convertible into shares in the legal person.

(6) Ownership interests can be so diversified that there may be no natural persons, whether acting alone or together, who ultimately control that legal person through ownership. In such a case, or where there is doubt as to whether any natural persons identified in 7.4.2.(2)(a) are beneficial owners, for the purposes of 7.4.2.(2)(b) examples of natural persons who ultimately control a legal person through other means could include those natural persons who exert control through personal connections (e.g. to those natural persons holding the positions detailed in paragraph 7.4.2.(5) above or that possess ownership); by participating in the financing of the enterprise; because of close intimate family relationships, historical or contractual associations; or as a result of default on certain payments.

(7) Finally, where no natural person is identified under either 7.4.2.(2)(a) or 7.4.2.(2)(b), the firm would identify and take reasonable measures to verify the identity of the natural person or persons who hold the position of senior managing officials of the legal person. In this respect, the senior managing official could be the natural person(s) responsible for strategic decisions that fundamentally affect the business or general direction of the legal person; or the natural person(s) who exercises executive control over the daily or regular affairs of the legal person through a senior management position, such as the chief executive officer, chief finance officer, managing or executive director, or president.

(8) In circumstances where a legal person is ultimately controlled by a trust, foundation or other legal arrangement, in accordance with paragraphs 21(4), 21(5) and 21(6) of Schedule 3, the firm shall identify, and take reasonable measures to verify the identity of, the beneficial owners and underlying principals of that trust, foundation or other legal arrangement. Sections 7.9. and 7.10. of this Handbook set out the measures to be taken by the firm in this regard.

(9) When identifying, and taking reasonable measures to verify the identity of, the beneficial owner or any underlying principal of a legal person as required by this section, 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.

Natural Persons

7.5. Legal Bodies Listed on a Stock Exchange

(1) In accordance with paragraph 4(5) of Schedule 3, the firm is not required to identify any shareholder, beneficial owner or underlying principal in relation to a customer, or a person which ultimately controls a customer, that is a company listed on a stock exchange prescribed by the [TBC] Regulations, or a majority owned subsidiary of such a company.

[TBC] Regulations

(2) 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 stock exchange prescribed by the [TBC] Regulations.

(3) The firm must, subject to section 9.5. of this Handbook, identify and verify those signatories with authority to operate an account or to give the firm instructions concerning the use or transfer of funds or assets of the legal body. In doing so the firm must act in accordance with the requirements of Schedule 3 and this Handbook for customers who are natural persons, including verifying the individual's authority to act in accordance with paragraph 4(3)(b) of Schedule 3.

Natural Persons

7.6. Protected Cell Companies

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

(2) 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 the prior written consent of the Commission.

(3) 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.

(4) Where a PCC is the customer, or beneficial owner or underlying principal, the firm must conduct CDD on both the core and the relevant PC(s), including the beneficial owners and underlying principals of such, and the directors of the core in accordance with the requirements for legal persons. While a PCC is a single legal entity, the beneficial owner of the core's shares and a PC's shares can be different and each must be identified and verified.

(5) The CDD measures for PCCs registered or authorised by the Commission as CISs under the POI Law can be found at section 7.16. of this Handbook.

Collective Investment Schemes Authorised or Registered by the Commission

(6) The CDD measures for PCCs which are licensed under the Insurance Business (Bailiwick of Guernsey) Law, 2002 as amended and where the beneficial owner of the relevant PC or PCC is a business which is listed on a stock exchange prescribed by the [TBC] Regulations (or by a majority owned subsidiary of such a listed business) are the same as those for legal persons listed on a stock exchange.

Legal Body Listed on a Stock Exchange

7.7. Incorporated Cell Companies

(1) An ICC is structured similarly to a PCC with a non-cellular core and an unlimited number of cells. 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.

(2) 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.

(3) 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.

(4) 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.

(5) Where an ICC or IC is the customer, or beneficial owner or underlying principal, the firm must conduct CDD on the relevant ICC or IC, including the beneficial owner and any underlying principal of the ICC or IC, in accordance with the requirements for legal persons.

(6) The CDD measures for ICCs or ICs registered or authorised by the Commission as CISs under the POI Law can be found at section 7.16. of this Handbook.

Collective Investment Schemes Authorised or Registered by the Commission

(7) The CDD measures for ICs or ICCs which are licensed under the Insurance Business (Bailiwick of Guernsey) Law, 2002 as amended and where the beneficial owner of the relevant IC or ICC is a business which is listed on a stock exchange prescribed by the [TBC] Regulations (or by a majority owned subsidiary of such a listed business) are the same as those for legal persons listed on a stock exchange.

Legal Body Listed on a Stock Exchange

7.8. Limited Partnerships and Limited Liability Partnerships

(1) 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, e.g. 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.

(2) An 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.

(3) Where an LP or LLP is the customer, or the beneficial owner or any underlying principal of a customer, the firm must identify and verify the identity of that LP/LLP, including as a minimum:

(a) the name of the LP/LLP, including any trading names;
(b) any official identification number;
(c) the nature and status of the LP/LLP;
(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);
(f) the powers that regulate and bind the LP/LLP;
(g) any natural or legal person(s) acting as GP (as applicable);
(h) any natural persons, e.g. underlying principals, authorised signatories or equivalent, with ultimate effective control over the capital or assets of the LP/LLP; and
(i) any person purporting to act on behalf of the LP/LLP, including his authority to so act.

(4) One or more of the following examples are considered suitable to verify aspects of the identity of the LP/LLP in accordance with Rule 7.8.(1):

(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, e.g. a search of a register of LPs/LLPs.

(5) Where the documents obtained are copies of the originals, the firm should refer to the requirements of chapter 6 of this Handbook.

Certification of Documentation for Legal Persons and Legal Arrangements

(6) The CDD measures for a customer which is an LP/LLP registered or authorised by the Commission as a CIS under the POI Law are set out in section 7.16. of this Handbook.

Collective Investment Schemes Authorised or Registered by the Commission

(7) The firm should take a risk-based approach when verifying the authorised signatories of an LP/LLP. Consideration should be given to the level of a signatory's authority and identifying which signatories will provide instructions to the firm and the type of instruction they are authorised to permit.

7.8.1. Understanding the Beneficial Ownership of Limited Partnerships and Limited Liability Partnerships

(1) Paragraph 4(3)(c) of Schedule 3 requires that the firm shall identify, and take reasonable measures to verify the identity of, the beneficial owner and any underlying principal of the LP/LLP and take measures to understand the ownership and control structure of that LP/LLP.

(2) When seeking to identify the beneficial owner and any underling principal of an LP the firm must act in accordance with the requirements for legal persons in Schedule 3 and the rules and guidance in section 7.4.2 of this Handbook.

Understanding the Beneficial Ownership of Legal Persons

(3) With regard to LLPs, in accordance with paragraph 21(2) of Schedule 3 and in turn as outlined in regulation 2 of the Beneficial Ownership Regulations, the firm shall identify, and take reasonable measures to verify the identity of, any person who holds, directly or indirectly, more than [TBC]% of the voting rights in the conduct and management of the LLP (whether pursuant to the members' agreement or section 14(3) of the LLP Law).

(4) When identifying, and taking reasonable measures to verify the identity of, the beneficial owner and any underlying principal of an LP/LLP as required by this section, 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.

Natural Persons

7.9. Foundations

7.9.1. Obligations of Businesses Establishing or Administering Foundations

(1) During the course of establishing a foundation relationship for which it is to act as foundation official, the firm must identify:

(a) the founder(s);
(b) all councillors;
(c) any guardian(s);
(d) any beneficiaries, including any default recipient; and
(e) any other natural person who exercises ultimate effective control over the foundation.

(2) When seeking to verify the identity of the beneficial owners and underlying principals of a foundation, the firm should refer to section 7.9.3. of this Handbook.

Understanding the Beneficial Ownership of Foundations

7.9.2. Obligations when Dealing with Foundations

(1) Where a foundation is the customer, or the beneficial owner or underlying principal of a customer, the firm must:

(a) identify and verify the identity of the foundation, including without limitation:
  (i) the full name;
  (ii) the legal status of the foundation;
  (iii) any official identification number (e.g. a registered number, tax identification number or registered charity or NPO number, where relevant);
  (iv) the date and country or territory of establishment/registration;
  (v) the registered office address and principal place of operation/administration (where different from the registered office);
  (vi) the powers that regulate and bind the foundation;
(b) identify and, subject to section 9.5. of this Handbook, verify the identity of any registered agent of the foundation;
(c) require the registered agent, foundation officials or other relevant person to notify the firm of the names of the beneficial owners and underlying principals, i.e.:
  (i) the founder(s), including any persons subsequently endowing the foundation;
  (ii) all councillors;
  (iii) any guardian(s);
  (iv) any beneficiaries, including any default recipient; and

(v) any other natural person who exercises ultimate effective control over the foundation; and

(d) understand the foundation structure and the nature and purpose of activities undertaken by the foundation sufficient to monitor such activities and to fully understand the business relationship or the purpose of the occasional transaction.

(2) One or more of the following examples are considered suitable to verify aspects of the identity of the 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.

(3) Where the documents obtained are copies of the originals, the firm should refer to the requirements of chapter 6 of this Handbook.

Certification of Documentation for Legal Persons and Legal Arrangements

(4) When seeking to verify the identity of the founder(s), councillors, guardian(s), beneficiaries and other parties identified by Rule 7.9.2.(1)(c), the firm should refer to Rule 7.9.2.(5) below and the following section 7.9.3. of this Handbook.

(5) Verification of the parties to a foundation must be undertaken either by the firm itself or, provided that the rules in chapter 10 of this Handbook are met, by requesting the registered agent or foundation official to provide the relevant information on the identity of such parties by way of a certificate or summary sheet.

Introduced Business

7.9.3. Understanding the Beneficial Ownership of Foundations

(1) In accordance with paragraph 4(3) of Schedule 3 and in turn as defined in Regulation 2 of the Beneficial Ownership Regulations, in relation to a foundation the firm shall identify, and take reasonable measures to verify the identity of, (without limitation):

(a) any natural person who holds, directly or indirectly, more than [TBC]% of the voting rights in the conduct and management of the foundation;
(b) any natural person who holds the right, directly or indirectly, to appoint or remove a majority of the officials of the foundation;
(c) any natural person who is a beneficiary in whom an interest has vested;
(d) any natural person who is the default recipient of the assets of the foundation in the event of its termination;
(e) any natural person who benefits from the foundation; and
(f) any founder or foundation official of the foundation.

(2) Other than where a business relationship has been assessed as high risk, the firm must take reasonable measures to verify the identity of any natural person falling within (a)-(e) of paragraph 7.9.3.(1) above prior to any distribution of foundation assets to (or on behalf of) that natural person.

(3) Where a business relationship has been assessed as being high risk, the firm must take reasonable measures to verify the identity of any natural person falling within (a)-(e) of paragraph 7.9.3.(1) above at the time that the assessment of risk is made. Where it is not possible to do so, e.g. because they are unborn or disenfranchised, the reasons must be documented and retained on the relevant customer's file.

(4) The firm must take reasonable measures to verify the identity of the underlying principals and other parties identified by Rules 7.9.1. or 7.9.2.(1)(c), e.g. any founder(s), foundation official(s), councillors, guardian(s) and any other person(s) with ultimate effective control over the foundation (including the beneficial owner or underlying principal of such an entity where it is a legal person or legal arrangement), before or during the course of establishing a business relationship or before carrying out an occasional transaction.

(5) When identifying the founder(s) in accordance with paragraph 4(3) of Schedule 3, the firm must identify, and take reasonable measures to verify the identity of, the initial founder(s) and any persons subsequently endowing the foundation after formation.

(6) Where a founder is a legal person or legal arrangement, the firm should identify and verify the identity of the founder in accordance with the relevant requirements of this chapter, including identifying and taking reasonable measures to verify the natural persons ultimately owning or controlling the founder.

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

(8) When verifying the identity of the founder(s), foundation official(s), beneficiaries and others as required by this section, 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.

Natural Persons

7.10. Trusts

7.10.1. Obligations of Trustees

(1) During the course of establishing a trust relationship for which it is to act as trustee, the firm must identify:

(a) the settlor(s);
(b) any protector(s), enforcer(s) and co-trustee(s);
(c) any beneficiary, whether his interest under the trust is vested, contingent or discretionary and/or any class of beneficiaries; and
(d) any other natural person who exercises ultimate effective control over the trust.

(2) Further information on the verification of the beneficial owners and underlying principals of a trust can be found in section 7.10.3. of this Handbook.

Understanding the Beneficial Ownership of Trusts

(3) In addition to the parties listed in Rule 7.10.1.(1), the firm must also gather and retain basic information on other regulated agents of, and service provides to, the trust. Examples of such include investment advisors or managers, accountants and tax advisors.

(4) For the purposes of Rule 7.10.1.(3), the following is deemed to constitute basic information:

(a) the full name of the regulated agent or service provider;
(b) their registered office address and principal place of business (where different from the registered office); and
(c) where a legal person, the names of any natural persons providing services to the trust.

7.10.2. Obligations when Dealing with Trusts

(1) Where a trust is the customer, or the beneficial owner or underlying principal of a customer, the firm must:

(a) identify and verify the identity of the trust, including without limitation:
  (i) the full name;
  (ii) any official identification number (e.g. a tax identification number or registered charity or NPO number, where relevant);
  (iii) the date and place of establishment of the trust; and
  (iv) the powers that regulate and bind the trust;
(b) identify and, subject to section 9.5. of this Handbook, verify the identity of the trustees of the trust;
(c) require the trustees of the trust to provide the firm with details of the identities of the beneficial owners and underlying principals, i.e.:
  (i) the settlor(s), including the initial settlor(s) and any persons subsequently settling funds into the trust;
  (ii) any protector(s), enforcer(s) and co-trustee(s);
  (iii) any beneficiaries, whether their interest under the trust is vested, contingent or discretionary and/or any class of beneficiaries; and
  (iv) any other natural person who exercises ultimate effective control over the trust; and
(d) understand the trust structure and the nature and purpose of activities undertaken by the trust sufficient to monitor such activities and to fully understand the business relationship or the purpose of the occasional transaction.

(2) When verifying the identity of the trust, subject to Rule 7.10.2.(3) below, the firm need not obtain copies of the entire trust instrument (e.g. trust deed or declaration of trust); obtaining copies of relevant extracts of such an instrument may suffice.

(3) Where the business relationship or occasional transaction has been assessed as high risk the firm must obtain:

(a) the entire trust deed together with any subsequent deeds of amendments and the letter(s) of wishes (where applicable); or
(b) relevant extracts of the trust deed, deeds of amendments and letter(s) of wishes (as applicable), together with an appropriate assurance from the trustee that the content of such documents does not contain contradictory information with other identification data gathered.

(4) Where documents obtained are copies of the originals, the firm should refer to the requirements of chapter 6 of this Handbook.

Certification of Documentation for Legal Persons and Legal Arrangements

(5) When seeking to verify the identity of the settlor(s), protector(s), enforcer(s), beneficiaries and other parties identified by Rule 7.10.2.(1)(c), the firm should refer to Rule 7.10.2.(6) below and the following section 7.10.3. of this Handbook.

(6) Verification of the parties to a trust must be undertaken either by the firm itself or, provided that the 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.

Introduced Business

7.10.3. Understanding the Beneficial Ownership of Trusts

(1) In accordance with paragraph 4(3) of Schedule 3, in relation to a trust the firm shall identify, and take reasonable measures to verify the identity of, (without limitation):

(a) any beneficiary who is a natural person, whether his interest under the trust is vested, contingent or discretionary;
(b) any other natural person who benefits from the trust;
(c) any natural person not within (a) or (b) above who exercises ultimate effective control over the trust; and
(d) any settlor, trustee , protector or enforcer of the trust.

(2) Other than where a business relationship 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, or any other natural person who benefits from, or exercises ultimate effective control over, the trust, prior to any distribution of trust assets to (or on behalf of) that natural person.

(3) Where a business relationship has been assessed as being high risk, the firm must take reasonable measures to verify the identity of all beneficiaries and other persons who are to benefit from, or exercises ultimate effective control over, the trust, at the time that the assessment of risk is made. Where it is not possible to do so, e.g. because they are unborn or disenfranchised, the reasons must be documented and retained on the relevant customer's file.

(4) 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 until such time that the trustee determines to make a distribution to the beneficiary and that beneficiary's interest in the trust property becomes vested.

(5) Schedule 3 recognises the differences between the interests of beneficiaries under discretionary trusts, as well as those under fixed interest trusts whose interests have not yet arisen and who are, therefore, contingent beneficiaries. In this respect Rule 7.10.3.(2) allows, other than in high risk scenarios, for the verification of the identity of a beneficiary to take place at the time that an interest is vested and a distribution of trust assets or property occurs to, or on behalf of, that beneficiary.

(6) Where the beneficiaries of a trust are designated by characteristics or by class, the firm should obtain sufficient information concerning the beneficiaries to satisfy itself that it will be able to establish the identity of a beneficiary at the time of a distribution or when the beneficiary gains vested rights, e.g. a beneficiary who is unaware of his beneficiary status until a point in time or a minor who attains age.

(7) The firm must take reasonable measures to verify the identity of the underlying principals, e.g. any settlor(s), trustee(s), protector(s) and enforcer(s) (including the beneficial owner or underlying

principal of such an entity where it is a legal person or legal arrangement), before or during the course of establishing a business relationship or before carrying out an occasional transaction.

(8) When identifying the settlor(s) in accordance with paragraph 4(3) of Schedule 3, the firm must identify, and take reasonable measures to verify the identity of, the initial settlor(s) and any persons subsequently settling funds into the trust.

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

(10) When verifying the identity of the settlor(s), trustee(s), protector(s), enforcer(s), beneficiaries and others as required by this section, 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.

Natural Persons

7.11. Charities and Non-Profit Organisations

(1) It is recognised that charities and NPOs are vulnerable to criminal and terrorist abuse. 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. This is of particular concern where the charity or NPO has connections with higher-risk countries or territories.

(2) Not all charities and NPOs are subject to scrutiny through legislation or registration requirements. Consequently a criminal or terrorist organisation can exploit the inherent risk in the vulnerabilities of 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.

(3) When carrying out a customer risk assessment as required by paragraphs 4(a) and 4(b) of Schedule 3 and section 3C of this Handbook, the following are example risk factors to be considered by the firm, both singly and cumulatively, when determining the risk rating of a charity or NPO:

(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 the nature of the projects (or equivalent) for which the charity or NPO provides funding; and
(e) the openness and transparency with which the charity or NPO conducts its affairs.

Risk Based Approach – Customer Risk Assessment

(4) Where a charity or NPO is the customer, the firm must:

(a) identify and verify the identity of the charity or NPO, including:
  (i) the full name;
  (ii) the primary address and mailing address (if different); and
  (iii) the date and place of establishment;
(b) understand the nature and purpose of the charity or NPO;

(c) identify, and take reasonable measures to verify the identity of, any natural persons, including underlying principals, authorised signatories or equivalent, with ultimate effective control over the management of the charity or NPO and the assets of the charity or NPO (if different); and

(d) identify, and verify the identity of, any person purporting to act on behalf of the charity or NPO, including verifying his authority to so act.

(5) The firm should also have policies, procedures and controls in place which seek to understand whether the charity or NPO is operated with transparency and integrity and has effective operational controls and an adequate governance or management function.

(6) Many jurisdictions require the registration of at least a sub-set of charities or NPOs for the purpose of ensuring the transparency of that jurisdiction's NPO sector. Whilst alone 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 lists of both registered charities and NPOs (excluding Sark).

Guernsey Registry - Charities & NPO Register

7.12. Sovereign Wealth Funds

(1) An 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.

(2) 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.

(3) Where an SWF is the customer, or beneficial owner or underlying principal, the firm must:

(a) identify and verify the existence of the SWF, including:
  (i) the name;
  (ii) the address;
  (iii) the date of establishment;
  (iv) the name of the national government; and
  (v) the investment powers;

(b) understand the legal standing of the SWF by reference to the applicable constitutional documents; and

(c) obtain the names of the authorised signatories and governing body (or committee, or equivalent) members and identify those natural persons with authority to give instructions over the use or transfer of funds or assets and verify the authority of those persons to so act.

(4) The firm must take reasonable measures to verify the identity of those natural persons identified by Rule 7.12.(3)(c). The extent of what is considered reasonable should be based on the risk attributed to the business relationship or occasional transaction and factors such as the nature, scale and complexity of the business being conducted.

Natural Persons

(5) Many SWFs are members of the 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.

(6) 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.

International Forum of Sovereign Wealth Funds

7.13. Life and Other Investment Linked Insurance

(1) Where the product or service provided by the firm is a life or other investment linked insurance policy, the firm must, in addition to identifying and verifying the customer, the beneficial owner and any underlying principal, also undertake the following measures on any beneficiary as soon as they are identified/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 arrangement; and

(b) for a beneficiary that is designated by characteristics or by class (e.g. a spouse or child) or by other means (e.g. 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.

(2) In accordance with paragraph 4(3)(f) of Schedule 3, the firm shall make a determination as to whether the beneficial owner or any beneficiary of a life or other investment linked insurance policy (at the point that a beneficiary is identified/designated) is a PEP.

(3) Where the firm determines that the beneficial owner or any beneficiary is a PEP, the firm must act in accordance with the requirements of paragraph 5 of Schedule 3 and section 8.10. of this Handbook.

Politically Exposed Persons

(4) Verification of the identity of any beneficiary identified in accordance with Rule 7.13.(1) must occur prior to any distribution to (or on behalf of) that beneficiary.

(5) When carrying out a customer risk assessment as required by paragraphs 4(a) and 4(b) of Schedule 3 and chapter 3 of this Handbook, the firm must include any beneficiary identified by Rule 7.13.(1) as a relevant risk factor in considering the risk of the business relationship or occasional transaction.

Risk Based Approach – Customer Risk Assessment

(6) Taking into account the requirements of Rule 7.13.(3), 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, any beneficial owner and underlying principal of the beneficiary prior to any distribution to (or on behalf of) the beneficiary.

Enhanced and Additional Customer Due Diligence

(7) When identifying and verifying the identity of a customer, beneficial owner and beneficiary as required by this section, the firm must act in accordance with the identification and verification requirements for customers who are natural persons, legal persons and legal arrangements.

Natural Persons

7.14. Employee Benefit Schemes, Share Option Plans or Pension Schemes

(1) 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 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, e.g. the administrator or the scheme manager, is considered as the principal and must be identified and verified by the firm in accordance with the requirements of this chapter.

(2) When carrying out a customer risk assessment as required by paragraph 3(a) or 3(b) of Schedule 3 and chapter 3 of this Handbook, the firm must include the natural or legal person identified by Rule 7.14.(1) as providing the funds as a relevant risk factor when determining the overall risk of the business relationship or occasional transaction.

Risk Based Approach – Customer Risk Assessment

(3) When identifying and verifying the identity of parties identified by Rule 7.14.(1), the firm must act in accordance with the identification and verification requirements for customers who are natural persons, legal persons and legal arrangements.

Natural Persons

7.15. Pooled Bank Accounts

(1) Banks often accept pooled deposits on behalf of professional firms and FSBs. These accounts may contain the funds of more than one underlying customer.

(2) Where the firm is licensed by the Commission under the Banking Supervision (Bailiwick of Guernsey) Law, 1994 as amended and has identified that an account operated by it on behalf of a specified business falls within one of sections (a)-(d) below, the firm may treat the specified business as its customer:

(a) a pooled account in the name of a fiduciary licensed by the Commission where the holding of funds in the pooled account is on a short-term basis;
(b) a client account in the name of a fiduciary licensed by the Commission or a firm of lawyers or estate agents registered with the Commission where the holding of funds in the client 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 licenced under the POI Law where the funds are subject to the Licensees (Conduct of Business) Rules 2016; and
(d) a client money account in the name of a firm licenced under the IMII Law where the funds are subject to the Insurance Managers and Insurance Intermediaries (Client Money) Regulations, 2008.

(3) Where the firm utilises the provisions of paragraph 7.15.(2), it must prepare and retain documentary evidence which confirms:

(a) that it has, subject to section 9.5. of this Handbook, undertaken CDD procedures in respect of the specified business, including ensuring that the specified business has appropriate AML and CFT policies, procedures and controls in place to identify and verify the underlying customers, including beneficiaries and underlying principals; and
(b) that the relationship relates solely to the provision of the products and services falling within paragraph 7.15.(2) above.

(4) Where the firm operates a pooled account on behalf of a professional firm or FSB which does not fall within one of sections (a)-(d) of paragraph 7.15.(2), the firm must identify and verify the identity of the customers, including any beneficial owner and underlying principal, for whom the professional firm or FSB is acting in accordance with the requirements of this Handbook.

(5) The firm should always consider whether the risks would be better managed if the firm undertook CDD on the beneficial owner and underlying principal(s) for whom the specified business is acting rather than treating the specified business as the customer.

(6) Where the firm considers that such action is necessary, e.g. because the firm has concerns in respect of the manner in which a pooled account is being used by a specified business, the firm must perform its own CDD measures on the underlying customers within the pooled account in accordance with the identification and verification requirements of Schedule 3 and this Handbook for natural persons, legal persons and legal arrangements.

Natural Persons

7.16. Collective Investment Schemes Authorised or Registered by the Commission

(1) Where the customer is a CIS authorised or registered by the Commission, the firm (other than where it has been nominated as the party responsible for undertaking investor CDD in accordance with section 4.7.1. of this Handbook) may consider the CIS to be the customer. In such cases it will be acceptable for the firm to identify only those natural persons holding a controlling ownership interest in the CIS.

(2) In order for the firm to consider the CIS as the principal to be identified and verified, it must obtain documentation which confirms the customer is a CIS authorised or registered by the Commission and, subject to paragraph 9.5.(7) of this Handbook, must identify the natural persons who have authority to operate an account or to give the firm instructions concerning the use or transfer of funds or assets and verify the authority of those persons to so act.

(3) With regard to the beneficial ownership of the CIS, the firm must seek written confirmation, either from the firm nominated in accordance with section 4.7.1. of this Handbook or the board (or equivalent) of the CIS, as to whether any natural person ultimately controls the CIS, either directly or indirectly, through ownership.

(4) For those natural persons holding a controlling ownership interest in the CIS, the firm must gather basic information on identity, including their legal name, residential address and date of birth.

(5) 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.

7.17. Non-Guernsey Collective Investment Scheme

(1) 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 NGCIS established outside the Bailiwick it may, in certain circumstances, place reliance on the administrator or transfer agent of the NGCIS to have undertaken CDD procedures on the investors.

(2) Where the firm provides management or custody services and wishes to rely on the CDD procedures of the administrator of the NGCIS, the firm must:

(a) undertake CDD procedures in respect of 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 requirements for high and low risk relationships;

(ii) contains adequate assurance that the administrator or transfer agent conducts the necessary CDD procedures in respect of investors (including the beneficial owners of such) into the NGCIS; and

(iii) contains an assurance that the administrator or transfer agent will notify the firm of any investor in the NGCIS, or the beneficial owner or underlying principal thereof, categorised as a PEP.

(3) 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.

(4) 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 undertake CDD on the investors into the NGCIS as if they were its customers in accordance with the requirements of section 4.7.2. of this Handbook.

Identifying and Verifying Investors in Collective Investment Schemes

(5) Where the firm is entering into a business relationship or conducting an occasional transaction with an NGCIS which is its customer, e.g. an accountant providing services to the NGCIS, the firm should treat the NGCIS as a legal person or legal arrangement and undertake CDD in accordance with the relevant sections of this chapter.

Chapter 8
Enhanced and Additional Customer Due Diligence

Contents of this Chapter

Schedule 3 Requirements

The requirements of Schedule 3 to the Law to which the Commission Rules and guidance in this chapter particularly relate are:

- Paragraph 3, which provides for a specified business to identify and assess the risks of ML and FT, both in respect of its business as a whole and its individual business relationships or occasional transactions. The paragraph also provides for a firm to ensure that its policies, procedures and controls are effective and appropriate to the assessed risk.

  Paragraph 3 Hyperlink

- Paragraph 4, which provides for the required CDD measures, when and to whom they should be applied.

  Paragraph 4 Hyperlink

- Paragraph 5, which provides for ACDD and ECDD measures in respect of business relationships and occasional transactions where the circumstances necessitate additional measures or the business relationship or occasional transaction has been assessed as high risk.

  Paragraph 5 Hyperlink

- Paragraph 8, which makes provisions in relation to anonymous accounts and shell banks.

  Paragraph 8 Hyperlink

- Paragraph 15, which makes provisions in relation to corporate governance and the review of compliance, including the requirement to appoint an FCCO.

  Paragraph 15 Hyperlink

8.1. Objectives

(1) This chapter relates to business relationships and occasional transactions which have been assessed as high risk, or involve one or more of the characteristics set-out in paragraph 5(2) of Schedule 3 and thus require the application of ACDD.

(2) This chapter should be read in conjunction with chapter 3 of this Handbook which provides guidance on the assessment of risk and with chapters 4 to 7 of this Handbook which provide for the standard CDD requirements.

8A. Additional Customer Due Diligence

8.2. Application of Additional Customer Due Diligence

(1) In addition to customers assessed by the firm as posing a high risk of ML and/or FT and for which ECDD is to be applied by the firm, there may be circumstances where the firm enters into or continues a business relationship, or undertakes an occasional transaction, with a customer which exhibits one or more of the characteristics prescribed in subparagraphs 5(2)(b)(i)-(iv) of Schedule 3 which are:

(a) the customer is not resident in the Bailiwick;
(b) the firm provides private banking services to the customer;
(c) the customer is a legal person or legal arrangement used for personal asset holding purposes;
(d) the customer is a company with nominee shareholders or that issues shares in bearer form.

(2) While the presence of one or more of these circumstances does not necessarily set the overall risk of the customer as standard or high risk, in accordance with paragraph 5(2) of Schedule 3 the firm shall undertake ACDD in order to mitigate the particular risks arising in the circumstances. This section of the Handbook sets out those additional steps to be taken.

8.3. Non-Resident Customer

(1) 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 typically have legitimate reasons for doing so. Some customers will, however, pose a risk of ML and/or FT and may be 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.

(2) Where the firm establishes or maintains a business relationship or undertakes an occasional transaction with a customer who is not resident in the Bailiwick, the firm must undertake one or more of the following ACDD measures in respect of that customer:

(a) understand the reason(s) behind the customer seeking to establish a business relationship or carry out an occasional transaction in the Bailiwick;
(b) use 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; and/or
(c) take reasonable measures to establish the source of funds and source of wealth of the customer (see section 8.9. of this Handbook).

(3) For the purposes of Rule 8.3.(2)(a), when determining the reasons for establishing a business relationship or undertaking an occasional transaction, the firm should document its determination, which should be more than merely 'tax planning', 'asset protection' or similar.

(4) 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 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.

8.4. Customer Provided with Private Banking Services

(1) Private banking is generally understood to be the provision of personalised banking and 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 and/or FT.

(2) Where the firm establishes or maintains a business relationship or undertakes an occasional transaction with a customer to which it provides private banking services, the firm must undertake one or more of the following ACDD measures in respect of that customer:

(a) review the business relationship on an annual basis, including all documents, data and information obtained under identification measures in order to ensure they continue to be appropriate and relevant;
(b) where monitoring thresholds are used, ensure that these are appropriate for the circumstances of the business relationship and consider whether they should be reduced to provide greater oversight of transactions connected with the business relationship; and/or
(c) take reasonable measures to establish the source of funds and source of wealth of the customer (see section 8.9. of this Handbook).

(3) Where the firm offers private banking services, it should consider on a case by case basis whether a customer utilises such services, or whether the products and/or services provided to the customer fall within more traditional retail banking services. In such circumstances ACDD would not be necessary.

8.5. Customer is an Asset Holding Vehicle

(1) Personal asset holding vehicles are legal persons or legal arrangements established by individuals for the specific purpose of holding assets for investment. Whilst there are perfectly legitimate reasons for establishing an asset holding vehicle, the use of such persons or arrangements may make identification of ultimate beneficial owners more difficult since layering of ownership can conceal the true sources of wealth or the controller of the investment.

(2) Where the firm establishes or maintains a business relationship or undertakes an occasional transaction with a customer which is a legal person or legal arrangement used for personal asset holding purposes, the firm must undertake one or both of the following ACDD measures in respect of that customer:

(a) determine the purpose and rationale for making use of such a vehicle and satisfy itself that the customer's use of such an asset holding vehicle has a genuine and legitimate purpose; and/or
(b) take reasonable measures to establish the source of funds and source of wealth of the customer (see section 8.9. of this Handbook).

(3) Rule 8.5.(2) applies where the asset holding vehicle is the customer, or where the asset holding vehicle is the third party for whom a trustee or general partner is acting as the customer.

(4) For the purposes of Rule 8.5.(2)(a), when determining the purpose and rationale for making use of an asset holding vehicle, the firm should document its determination, which should be more than merely 'tax planning', 'asset protection' or similar.

8.6. Customer with Nominee Shareholders or the Ability to Issue Bearer Shares

8.6.1. Nominee Shareholders

(1) 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. It thus presents a higher risk scenario, making it more difficult for the firm to establish the true beneficial ownership of a customer.

(2) Where the firm establishes or maintains a business relationship or undertakes an occasional transaction with a customer which is a legal person with nominee shareholders, the firm must undertake one or both of the following ACDD measures in respect of that customer:

- (a) determine and satisfy itself as to the reasons why the customer is making use of nominee shareholders; and/or
- (b) use 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.

8.6.2. Bearer Shares

(1) When assessing the risk of a particular business relationship or occasional transaction, the firm should consider whether any legal person who is the customer, beneficial owner or underlying principal has issued or has the potential to issue bearer shares, bearer warrants or bearer negotiable instruments.

(2) 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, e.g. 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(s) of a bearer share or more broadly bearer share companies.

(3) Where the firm's risk appetite allows for a customer, or beneficial owner or underlying principal, to have issued or have the ability to issue bearer shares, the firm must have appropriate procedures and controls in place, including the application of ACDD, to ensure that they are not misused for ML and/or FT. The procedures should apply irrespective of whether the identified bearer share represents an amount below the relevant threshold for ownership or control of the legal person.

(4) Where the firm establishes or maintains a business relationship or undertakes an occasional transaction with a customer which is a legal person and has issued, or has the ability to issue, bearer shares, the firm must undertake all of the following ACDD measures in respect of that customer:

- (a) determine and satisfy itself as to the reasons why the customer has issued bearer shares or retains the ability to do so;
- (b) have custody of the bearer shares or be satisfied as to the location and immobilisation of the bearer shares. This should include confirming the number and location of the bearer shares with the customer on a periodic basis, or receiving a written undertaking from the custodian

that the firm will be notified of any changes to records relating to those shares and the custodian;

(c) ensure that any new or continued relationships or any occasional transactions are approved by the senior management of the firm; and

(d) review the business relationship on at least an annual basis, including all documents, data and information obtained under identification measures to ensure that they remain appropriate and relevant.

8B. Enhanced Customer Due Diligence

8.7. Application of Enhanced Customer Due Diligence

(1) In addition to customers assessed by the firm as posing a high risk of ML and/or FT, there may be circumstances where the firm enters into or continues a business relationship, or undertakes an occasional transaction, with a customer which exhibits one or more of the mandatory high risk factors listed in paragraph 5 of Schedule 3 and to whom ECDD must be applied.

(2) As referenced above, in accordance with paragraph 5 of Schedule 3, the firm shall undertake ECDD in the following circumstances:

(a) a business relationship or occasional transaction in which the customer or any beneficial owner or underlying principal is a foreign PEP;

(b) a business relationship which is a correspondent banking relationship, or similar to such a relationship in that it involves the provision of services, which themselves amount to specified business or facilitate the carrying out of such business, by one specified business to another;

(c) a business relationship or occasional transaction where the customer is established or situated in a country or territory that –

(i) provides funding or support for terrorist activities, or does not apply (or insufficiently applies) the FATF Recommendations; or

(ii) is a country otherwise identified by the FATF Recommendations as a country for which such measures are appropriate;

(d) a business relationship or occasional transaction 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; or

(e) a business relationship or occasional transaction which has been assessed by the firm as a high risk relationship.

(3) This section sets out the requirements and provides guidance in respect of the treatment of customers which have been assessed by the firm as posing a high risk or are required to be subject to ECDD in accordance with the requirements of paragraph 3 of Schedule 3.

8.8. Policies, Procedures and Controls

(1) Where the firm has assessed, taking into account the high risk indicators provided in chapter 3 of this Handbook, that the business relationship or occasional transaction is high risk – whether because of the nature of the customer, their location, or because of the delivery channel or the product/service features available – the firm must ensure that its policies, procedures and controls require ECDD measures to be undertaken as required by paragraph 5 of Schedule 3.

(2) It may be that CDD measures routinely applied already address some of the risk characteristics of high risk customers (e.g. the verification of beneficial owner(s) and understanding the nature and purpose of the relationship). Nevertheless, the ECDD must be in addition to the measures taken in respect of other business relationships or occasional transactions and must address the particular risk(s) presented by the customer.

(3) Where the firm has determined that ECDD is required for a business relationship or occasional transaction, in accordance with paragraph 5 of Schedule 3 the firm shall, as a minimum:

(a) obtain senior management approval for establishing the business relationship or occasional transaction;
(b) obtain senior management approval for, in the case of an existing business relationship with a foreign PEP, continuing that relationship;
(c) take reasonable measures to establish the source of any funds and of the wealth of the customer and beneficial owner and underlying principal (see section 8.9. of this Handbook);
(d) carry 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 (see chapter 11 of this Handbook); and
(e) take one or more of the following steps as would be appropriate to the particular business relationship or occasional transaction:
    (i) obtaining additional identification data (see section 5.2. of this Handbook);
    (ii) verifying additional aspects of the customer's identity (see section 5.3. of this Handbook); and/or
    (iii) obtaining additional information to understand the purpose and intended nature of the business relationship or occasional transaction.

(4) In addition to the minimum requirements of paragraph 5 of Schedule 3 as noted above, below are examples of further steps that the firm could take as part of its ECDD measures to address specific risks arising from a high risk business relationship or occasional transaction:

(a) update more regularly the identification data held on the customer and beneficial owner;
(b) obtain information on the reasons for intended or performed transactions;
(c) in the case of an existing business relationship which has been assessed as high risk not involving a foreign PEP, obtain senior management approval for continuing that relationship;
(d) require the first payment to be carried out through an account in the customer's name with an Appendix C business;
(e) commission 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 any beneficial owner or underlying principal; and/or
(f) obtain internal information obtained from group representatives or offices based in a jurisdiction where the customer has a connection.

8.9. Source of Funds and Source of Wealth

(1) Establishing and understanding the customer's source of funds and source of wealth are important aspects of the due diligence process, especially in respect of business relationships or occasional transactions involving foreign PEPs.

(2) In accordance with subparagraph 5(3)(a)(iii) of Schedule 3, as part of its ECDD procedures the firm shall take reasonable measures to establish the source of funds and source of wealth of a customer.

(3) In complying with the aforementioned requirement of Schedule 3, the firm must establish the source of funds and source of wealth of the customer together with any beneficial owners or underlying principals, particularly those providing funds, assets or any other form of value to the customer, business relationship or occasional transaction.

(4) 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 a person both within and outside a business relationship, i.e. those activities which have generated a customer's net assets and property.

(5) The firm must, in establishing the source of any funds or wealth, document and evidence consideration of the risk implications of the source of the funds and wealth and the geographical sphere of the activities that have generated a customer's source of funds and/or wealth.

(6) Measures the firm could take to establish the source of funds and source of wealth could include:

(a) commission an independent and reliable report from a specialist agency about the source of funds involved and/or the source of the customer's overall wealth;
(b) obtain reliable information directly from the customer concerned, e.g. by 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, obtain reliable information about the source of funds involved and/or the source of the customer's overall wealth from another member of the group where the customer has a connection;
(d) obtain information from a reliable third party (e.g. a professionally qualified solicitor, accountant or tax advisor) who has an office in a country or territory connected with the customer about the source of the customer's funds involved in the business relationship or transaction and/or the source of the customer's overall wealth;
(e) where the customer has been introduced to the firm, obtain information about the source of funds involved and/or the customer's source of wealth from the introducer;
(f) where information is publicly available or available through subscription databases, obtain information about the source of funds involved and/or the source of the customer's overall wealth from a reliable public or private source; or
(g) obtain information from financial statements that have been prepared and audited in accordance with generally accepted accounting principles.

(7) For the firm to accept a customer's responses on an application form at face value, particularly where vague responses are given, e.g. 'employment' or 'salary', without further clarification, such as where the customer was employed and his actual level of income would not be considered as having taken reasonable measures to establish the source of funds and source of wealth.

(8) The requirements in respect of establishing the source of a customer's funds are on-going and apply to all new proceeds passing through the relationship, either from the customer or a third party. Monitoring undertaken as part of ECDD should include assessing on an ongoing basis whether the transactional activity of that relationship is consistent with the risk profile of that customer, including his source of wealth.

8.10. Politically Exposed Persons

8.10.1. Introduction

(1) 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 terrorist financing. Where a PEP also has connections to countries or business sectors where corruption is widespread, the risk is further increased.

(2) PEP status itself does not incriminate individuals or entities. It will mean, however, that a customer who is a foreign PEP is subject to ECDD measures and that a domestic PEP may on the basis of risk be subject to ECDD measures. The nature and scope of the firm's activities, together with the results of its business risk assessment and risk appetite, will determine whether the existence of PEPs is a practical issue for the firm.

(3) 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.

8.10.2. Identification of Politically Exposed Persons

(1) Paragraph 5(4) of Schedule 3 defines three main categories of PEP:

(a) "foreign PEP" – a 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 person who holds or has held or has been elected or appointed to a prominent public function within the Bailiwick; and
(c) "international organisation PEP" – a person who is or has been entrusted with a prominent function by an international organisation.

(2) In order to determine whether a customer, or beneficial owner or underlying principal, is a PEP, the firm must consider:

(a) assessing countries which pose the highest risk of corruption (one source of information is the Transparency International Corruption Perception Index), establishing those natural persons who are the current and former holders of prominent public functions within those high risk countries and determining, as far as is reasonably practicable, whether or not a customer, or beneficial owner or underlying principal, has any connections with such individuals. The UN, the European Parliament, the UK Foreign and Commonwealth Office, and the Group of States Against Corruption may be useful information sources;
(b) seeking confirmation from a customer, or beneficial owner or underlying principal, e.g. through a question within an application, as to whether they hold, or have held, a prominent public function either within the Bailiwick or beyond, or for an international organisation; or
(c) using commercially available databases to identify such persons.

(3) Where the firm identifies that an individual who is the customer, or beneficial owner or underlying principal to a business relationship or occasional transaction, is a foreign PEP, it shall apply ECDD measures to that business relationship or occasional transaction in accordance with paragraph 5 of Schedule 3.

(4) Where the firm identifies that a customer, or any beneficial owner or underlying principal, 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 risk assessment of the business relationship or occasional transaction conducted in accordance with paragraph 3 of Schedule 3 and the rules in chapter 3 of this Handbook.

(5) Where, having conducted a customer risk assessment, the firm concludes that the business relationship or occasional transaction is high risk, the firm must apply ECDD measures in accordance with paragraph 5(3)(a) of Schedule 3 and section 8.8 of this Handbook.

(6) 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. Instead the firm can apply CDD (and where required ACDD) measures where the firm considers this appropriate.

(7) Where the firm identifies that a foreign, domestic or international organisation 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 a beneficial owner or underlying principal and where no property of that PEP is handled in the particular business relationship or occasional transaction, the firm should undertake a risk assessment of the relationship, including consideration of the nature of the PEP's role and reason why the PEP holds such a role.

(8) 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 should apply CDD (and ACDD) appropriate to the form of the customer in accordance with chapters 4 to 7 of this Handbook.

(9) One such example would be a UK county council pension scheme investing in a closed-ended private equity partnership where the members of the pension committee are PEPs through their roles as county councillors but where they do not exercise ultimate effective control over the customer. Those persons have no economic interest in the funds involved in the business relationship or occasional transaction (beyond their pension rights as a resident of that county) and the risk of the relationship being used as a vehicle for the laundering of any personal funds is minimal.

8.10.3. Family Members and Close Associates

(1) 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 or close associate of such 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.

(2) In this respect the definition of a PEP set out in paragraph 5 of Schedule 3 includes an immediate family member or close associate. The scope of these two terms is not categorically defined, as the interpretation of them 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 and close associates is fluid and may change over time.

(3) In deciding whether a person is an immediate family member or close associate, the firm should determine the extent of the influence that a particular relationship or association has and assess the level of risk that exists through the particular connection with a PEP.

(4) For immediate family members, 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.

(5) For close associates, paragraph 5 of Schedule 3 provides two mandatory examples; however there may be additional instances where the firm considers a person to be a close associate. These could include known partners outside the family unit (e.g. girlfriends, boyfriends and mistresses) or prominent members of the same political party, civil organisation, labour or employee union as the PEP. 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.

(6) In deciding whether a person is a family member or close associate of a PEP, the firm need only research information which is in its possession or which is publicly available.

8.10.4. International Organisation PEPs

(1) In accordance with paragraph 5(4)(d) 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 i.e. directors, councillors and members of the board or equivalent functions of an international organisation.

(2) 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.

(3) Examples of international organisations covered by Schedule 3 and this Handbook include the UN, the World Bank and NATO.

8.11. Correspondent Relationships

(1) A correspondent relationship is the provision of a financial service, e.g. banking services, by one entity (the "correspondent institution") to another entity (the "respondent institution"). Used by banks and other FSBs throughout the world, correspondent accounts enable the firm to conduct business and provide services to its customers that it does not offer directly.

(2) In relation to correspondent relationships for banking and those established for securities transactions or funds transfers, whether for the firm as principal or for its customers, the firm must take additional steps in relation to CDD including those in (a) to (e) below and, where relevant, those in the following rule:

(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 or FT 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, i.e. sign-off before establishing new correspondent relationships; and

(e) document the respective AML and CFT responsibilities of each institution.

(3) Where a correspondent relationship involves the maintenance of 'payable-through accounts', the firm must also take steps in order to satisfy itself that:

(a) it clearly understands the respective responsibilities of each institution;
(b) the customer (the respondent institution) has complied with all of the required CDD obligations set out in Schedule 3 and this Handbook on those of its customers with direct access to the accounts of the correspondent institution; and
(c) the respondent institution is able to provide relevant customer identification data upon request to the correspondent institution.

(4) The firm must ensure that appropriate and effective policies, procedures and controls are in place when establishing a correspondent relationship with a foreign bank and other institution.

(5) 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.

8.12. High Risk Countries or Territories

(1) In accordance with paragraph 5 of Schedule 3, the firm shall apply ECDD measures to a business relationship or occasional transaction where the customer is established or situated in a country or territory which:

(a) provides funding or support for terrorist activities;
(b) does not apply or insufficiently applies the FATF Recommendations; or
(c) has otherwise been identified by the FATF Recommendations as a country for which such measures are appropriate.

(2) The firm must have a policy in place which enables it to determine those countries or territories falling within (a) to (c) above. As part of this policy, the firm must be aware of concerns about weaknesses in the AML and CFT systems of other countries or territories.

(3) When determining which countries or territories its policy and associated procedures and controls should apply to, the firm must consider:

(a) Business from Sensitive Sources Notices and Instructions issued from time to time by the Commission;
(b) findings of reports issued by the FATF, FATF-style regional bodies, FATF associate members such as: MONEYVAL; the Asia/Pacific Group on Money Laundering; the Group of International Finance Centre Supervisors; Transparency International; the IMF; and the World Bank (see Appendix B);
(c) situations where the country or territory has not been the subject of an AML and CFT assessment; and
(d) its own experience, or the experience of other group entities where part of a multinational group, which may have indicated weaknesses or trends in other countries or territories.

Chapter 9
Simplified Customer Due Diligence

Contents of this Chapter

Schedule 3 Requirements

The requirements of Schedule 3 to which the Commission Rules and guidance in this chapter particularly relate are:

- Paragraph 3, which provides for a specified business to identify and assess the risks of ML and FT, both in respect of its business as a whole and its individual business relationships or occasional transactions. Schedule 3 also provides for a firm to ensure that its policies, procedures and controls are effective and appropriate to the assessed risk.

  Paragraph 3 Hyperlink

- Paragraph 4, which provides for the required CDD measures, when and to whom they should be applied.

  Paragraph 4 Hyperlink

- Paragraph 6, which provides for SCDD measures to be applied to business relationships which have been identified as being low risk relationships.

  Paragraph 6 Hyperlink

- Paragraph 15, which makes provisions in relation to corporate governance and the review of compliance, including the requirement to appoint an FCCO.

  Paragraph 15 Hyperlink

9.1. Introduction

(1) This chapter provides for the treatment of business relationships and occasional transactions which have been assessed as low risk pursuant to paragraph 3 of Schedule 3 and chapter 3 of this Handbook. It sets out the ability to apply SCDD to business relationships or occasional transactions in specific circumstances and defines those simplified measures which can be applied.

Risk Based Approach

(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 customer.

9.2. Simplified Customer Due Diligence Measures

(1) The general rule is that business relationships and occasional transactions are subject to the full range of CDD measures as identified by 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, any beneficial owner and underlying principal.

(2) There may however be circumstances where the risks of ML and FT have been assessed by the firm as being low. Examples could include:

(a) a locally resident customer where the purpose and intended nature of the business relationship or occasional transaction is clearly understood by the firm and where no aspect of the business relationship or occasional transaction is considered to carry a high risk of ML and FT;
(b) where the risks associated with the relationship are inherently low and information on the identity of the customer, and any beneficial owner and underlying principal, is publicly available; or
(c) where adequate checks and controls exist elsewhere in publicly available systems.

(3) There may also be circumstances where the risk of ML and FT occurring has been assessed as low by the Bailiwick as part of its NRA.

National Risk Assessment [TBC]

(4) In such circumstances the firm may consider applying SCDD measures when identifying, and verifying the identity of, the customer, and any beneficial owner and underlying principal.

(5) The simplified measures should be commensurate with the lower risk factors, e.g. they should relate only to relationship acceptance measures or to aspects of ongoing monitoring. Examples of possible measures could include:

(a) reducing the frequency of customer identification updates;
(b) reducing the degree of on-going monitoring and scrutinising 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, but inferring the purpose and nature from the type of transactions or business relationship established.

(6) The firm must ensure that, when it becomes aware of circumstances which affect the assessed risk of the business relationship or occasional transaction, a review of the identification data held is undertaken to determine whether it remains appropriate to the revised risk of the business relationship or occasional transaction.

(7) 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 having regard to the relationship and the risks of ML and FT.

(8) Where the risk has been assessed as anything other than low, the firm must not apply SCDD measures.

9.3. Bailiwick Residents

(1) Where the firm is establishing a business relationship or undertaking an occasional transaction with a customer who is a natural person resident in the Bailiwick, it may apply SCDD measures provided the requirements as set out above are met. Where the firm has determined that it can apply SCDD because the risks have been assessed as low, it may elect to verify one of points (b): date of birth and (c): residential address under Rule 5.3.(1) of this Handbook, in addition to (a): legal name.

(2) Notwithstanding the above, it should be borne in mind that not all Bailiwick residents are intrinsically low risk. The firm must ensure that a risk assessment of the business relationship or occasional transaction is undertaken in accordance with the requirements of paragraph 3 of Schedule 3 and that where the relationship is considered to be other than low risk, that the relevant CDD/ECDD is undertaken as applicable.

9.4. Bailiwick Public Authorities

(1) Where the firm is establishing a business relationship or undertaking an occasional transaction with a Bailiwick public authority, it may choose to apply SCDD measures. In this respect, where SCDD is undertaken, it is not necessary to apply full identification measures on the authority and any controllers of the authority.

(2) The firm must obtain at a minimum the following information about the public authority:

(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, signatories and authorised officials of the public authority.

(3) 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.

(4) Where a natural person authorised to act on behalf of a Bailiwick authority is acting in the course of employment, it is not necessary to identify and verify the identity of such persons; however the firm should confirm the natural person's authority to so act.

9.5. Appendix C Business

(1) 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 standards to combat ML and FT consistent with the FATF Recommendations and where such businesses are appropriately supervised for compliance with those requirements.

(2) The fact that a country or territory has requirements to combat ML and FT that are consistent with the FATF Recommendations means only that the necessary legislation and other means of ensuring compliance with the FATF Recommendations is 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.

(3) The inclusion of a country or territory in Appendix C does not mean that country or territory is intrinsically low risk, nor does it mean that any business or customer arising from or connected with such a country is to be automatically treated as low risk.

(4) Where a customer, or a beneficial owner or underlying principal, has been identified as an Appendix C business, the purpose and intended nature of the relationship is understood and any beneficial owner of the Appendix C business has been identified, verification of the identity of the Appendix C business and any beneficial owner is not required.

(5) If the Appendix C business is acting for or on behalf of another party, subject to the provisions of sections 4.7.2.2. and 7.15. of this Handbook, that third party must be identified and their identity verified in accordance with the requirements of Schedule 3 and this Handbook.

(6) Where the Appendix C business is a specified business supervised by the Commission, the identification of any beneficial owner of the Appendix C business is not required, other than where the firm considers this appropriate based upon the circumstances of the business relationship or occasional transaction.

(7) Where a 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. 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 fund.

(8) 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 should use commercial judgement in considering whether or not to deal with a regulated FSB or PB and may, if it wishes, impose higher standards than the minimum standards identified in this Handbook.

9.5.1. Determination of Appendix C Countries and Territories

(1) The Commission makes its determination of Appendix C jurisdictions based on the consideration of several factors including:

(a) the jurisdiction's membership of FATF and/or a FATF-style regional body;
(b) reports and assessments by FATF and/or other regional body for compliance with the FATF Recommendations;
(c) good governance indicators;
(d) the likely level of co-operation the Commission could expect to receive from the competent authorities within the country or territory;

(e) the level of drug trafficking, bribery and corruption and other financial and organised crime within the jurisdiction; and
(f) the extent of terrorism and terrorist financing activities within the jurisdiction.

(2) When reviewing assessments undertaken by the FATF or other FATF-style regional bodies of a country or territory's compliance with the FATF Recommendations, particular attention is given to whether:

(a) the country or territory is compliant or largely compliant with FATF Recommendations (in particular Recommendations 10, 11 and 12); and
(b) the country or territory's AML and CFT regime has been assessed as highly or substantially effective against the FATF's eleven 'Immediate Outcomes' set out within its methodology for compliance with the FATF Recommendations.

9.6. Receipt of Funds as Verification of Identity

(1) Where the customer, and any beneficial owner and underlying principal, 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.

(2) 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 underlying principal;
(c) payments are only paid to an account in the customer's name (i.e. no third party payments allowed);
(d) payments are only paid to an account in the customer's name, 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;
(e) no changes are made to the product or service that enable funds to be received from or paid to third parties; and
(f) no cash withdrawals are permitted other than by the customer, or an underlying principal, on a face-to-face basis where identity can be confirmed, and in the case of significant cash transactions, reasons for cash withdrawal are verified.

(3) The firm must ensure that, once a relationship has been established, should any of the conditions set out in Rule 9.6.(2) no longer be met, full verification of the identity of the customer, and any beneficial owner and underlying principal, is carried out in accordance with the requirements of Schedule 3 and this Handbook.

(4) 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 standard CDD requirements, it must ensure that receipt of funds is not used to verify the identity of the customer, or any beneficial owner or underlying principal.

(5) The firm must retain documentary evidence to demonstrate the reasonableness of its conclusion that the risks of ML and FT inherent in the business relationship being established or the occasional transaction being undertaken are low.

Chapter 10
Introduced Business

Contents of this Chapter

Schedule 3 Requirements

The requirements of Schedule 3 to the Law to which the Commission Rules and guidance in this chapter particularly relate are:

- Paragraph 4, which provides for the required CDD measures, when and to whom they should be applied.

  Paragraph 4 Hyperlink

- Paragraph 10, which provides for the CDD measures to be undertaken in introduced business relationships.

  Paragraph 10 Hyperlink

- Paragraph 15, which makes provisions in relation to corporate governance and the review of compliance, including the requirement to appoint an FCCO.

  Paragraph 15 Hyperlink

10.1. Introduction

(1) An introduced business relationship 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 with a specified business on behalf of that customer. Introducer relationships may be business relationships 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 7.15. of this Handbook.

Pooled Bank Accounts

(3) This chapter does not apply to outsourcing arrangements. In 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 ongoing periodic testing. This contrasts with an outsourced arrangement where the outsourced service provider applies the CDD measures on behalf of the delegating firm in accordance with the delegating firm's procedures and is subject to oversight and control of the effective implementation of those procedures by the delegating firm.

10.2. Risk Exposure

(1) Introduced business by its very nature has the capacity to be high risk. While the firm is still required to hold sufficient identifying information about its customer, and any beneficial owner or underlying principal, the firm places reliance on a third party to have adequately and appropriately verified that customer and connected parties.

(2) The firm must recognise the increased risk posed by introducer relationships and ensure that its consideration of these risks is adequately documented within its business risk assessments.

(3) In addition to an explanation of any risks identified within its introducer arrangements, the firm's assessment should also include a description of the policies, procedures and controls established to mitigate such risk.

(4) The firm must use a risk-based approach when deciding, on a customer by customer basis, whether it is appropriate to rely on a certificate or summary sheet from an introducer for a customer in accordance with paragraph 10 of Schedule 3 or whether it considers it necessary to do more.

(5) In accordance with Schedule 3 the ultimate responsibility for CDD measures will remain, as always, with the board of the firm.

10.3. Establishing an Introducer Relationship

(1) When establishing an introducer relationship the firm must satisfy itself that the introducer:

(a) has appropriate risk-grading procedures in place to differentiate between the CDD requirements for high and low risk relationships;
(b) conducts appropriate and effective CDD procedures in respect of its customers, including ECDD measures for PEPs and other high risk customers; and
(c) has appropriate record keeping requirements as set out in paragraph 14 of Schedule 3.

(2) Paragraph 10 of Schedule 3 requires that where the firm places reliance on a third party, it shall obtain written confirmation of identity from the introducer, by way of a certificate or summary sheet(s), detailing the elements of the CDD process set out in subparagraphs 4(3)(a) – (d) of Schedule 3.

(3) The CDD process referred to in paragraph 10.3.(2) above includes the following elements:

(a) identifying the customer by name and verifying that customer's identity using reliable, independent source documents, data or information;
(b) identifying any beneficial owner and underlying principal (in the case of a trust, the beneficiaries as beneficial owners and the settlors, trustees and the protector as underlying principals) and taking reasonable measures to verify the identity of any beneficial owner or underlying principal by name such that the firm is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements this includes the firm understanding the ownership and control structure of the customer, identifying any beneficial owner and underlying principals, directors, authorised signatories or equivalent, with ultimate effective control over the capital assets of the legal person;
(c) determining whether the customer is acting on behalf of another person and taking reasonable steps to obtain sufficient identification data to identify and verify the identity of that other person; and
(d) understanding and, as appropriate obtaining information on, the purpose and intended nature of the business relationship.

(4) A template certificate which may be used by the firm for introduced business can be found here:

Introduced Business Certificate

(5) The firm must take adequate steps to be satisfied that the introducer will supply, upon request without delay, certified copies or originals of the identification data and other evidence it has collected under the CDD process.

(6) Where an introduced relationship presents a higher risk of ML or FT, consideration should be given to whether it is appropriate to rely solely upon the information provided by the introducer or whether supplemental CDD information and/or documentation is required.

(7) The firm must not place reliance upon an introducer where it suspects ML and/or FT in connection with the customer or any beneficial owner or underlying principal.

(8) It is the responsibility of the introducer to inform the firm of any changes to the parties involved in an introducer arrangement, e.g. 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 without delay.

10.4. Testing

(1) The firm must have a scheduled programme of testing to ensure that on an on-going basis introducers are able to fulfil the requirement that certified copies or originals of the identification data will be provided, upon request, without delay. This will involve the firm adopting ongoing procedures to ensure it has the means to obtain that identification data.

(2) The testing programme should be risk-based and commensurate with the risk exposure, size and scope of the business introduced. The programme should act as an appropriate and effective control to allow the firm to be confident that it can continue to rely upon an introducer to fulfil its obligations. 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.

(3) 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.

(4) The scope of the testing undertaken should include verification that the information received on the introducer certificate or summary sheet containing information about the underlying customer, beneficial owner or underlying principal, 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.

(5) For the purposes of Rule 10.4.(1), 'without delay' should be interpreted as an introducer providing a response within two business days following a formal request by the firm.

(6) 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 without delay if requested to do so, the firm must apply CDD measures in accordance with paragraph 4 of Schedule 3 for that customer and give consideration to terminating its relationship with the introducer.

10.5. Termination

(1) In the event that an introducer terminates its relationship with an introduced customer, the firm should consider how best it can continue to maintain compliance with the CDD obligations for that customer. In this respect the firm should give consideration to the following:

(a) instructing the introducer to provide the firm with copies of the relevant evidence of identity held; or
(b) gathering its own identification data on the customer and terminating the introducer relationship.

10.6. Group Introducers

(1) 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 to be re-verified, provided that the group entity acting as introducer provides the firm with written confirmation that it:

(a) applies CDD requirements in line with paragraph 4 of Schedule 3;
(b) meets the requirements of paragraph 10 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 and other relevant documentation relating to the CDD requirements upon request and without delay. This requirement is satisfied if the firm has access to the information electronically via a group-wide database.

(2) The firm must not regard group introduced business as intrinsically low risk and must use a risk-based approach when deciding 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 customer identification and verification remains with the firm.

10.7. Chains of Introducers

(1)	Chains of introducers are not permitted and the firm must not place reliance on an introducer which forms part of a chain.

(2) This avoids a situation whereby, should the middle institution fall away, the receiving business would be left with difficulty in 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

Schedule 3 Requirements

The requirements of Schedule 3 to the Law to which the Commission Rules and guidance in this chapter particularly relate are:

- Paragraph 11, which provides for the monitoring of transactions and other activity and for conducting ongoing CDD.

  Paragraph 11 Hyperlink

- Paragraph 15, which makes provisions in relation to corporate governance and the review of compliance, including the requirement to appoint an FCCO.

  Paragraph 15 Hyperlink

11.1. Introduction

(1) The ongoing 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 also vital that the firm understands a customer's background and is aware of changes in the customer's circumstances 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 and/or FT 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) It should be borne in mind that there are two strands to effective ongoing monitoring. The first relates to the transactions and activity which occur on a day-to-day basis within a 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. The second strand 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 and underlying principals. This is achieved through maintaining relevant and appropriate identification data for the customer.

(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, unusual or complex transactions or activity so that ML and FT may be identified and prevented.

11.2. Objectives

(1) A key prerequisite to managing the risk of a business relationship or occasional transaction is understanding the customer (and any beneficial owner and underlying principal) and where changes to those parties occur. Also critical is maintaining a thorough understanding of the customer and appropriately monitoring a customer's transactions in order to be in a position to detect and subsequently report suspicious activity. 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 assessment 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.

(2) The monitoring of business relationships should involve the application of scrutiny to large, unusual or complex transactions, patterns of transactions or activity to ensure that such transactions 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 customers (including foreign PEPs) and jurisdictions, high risk business relationships and high risk transactions.

(3) 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, e.g. unusual patterns of transactions with no apparent or visible economic or lawful purpose.

(4) 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

(1) The firm must monitor the transactions and activity associated with its customers on the basis of a risk-based approach, with high risk customers and PEPs being subjected to an appropriate frequency of scrutiny, which must be greater than that scheduled for other customers.

(2) This approach will generally mean more frequent or intensive monitoring, including greater scrutiny of:

(a) high risk customers, particularly those involving PEPs;
(b) high risk products/services;
(c) high risk countries or territories; and
(d) sanctioned entities.

(3) Examples of the additional monitoring arrangements for high risk customers could include:

(a) undertaking more frequent reviews of high risk customers 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, e.g. the FCCO;
(e) ensuring that the firm has adequate management information systems to provide the board and FCCO with timely information needed to identify, analyse and effectively monitor higher risk customers and accounts;
(f) appropriate approval procedures for high value transactions in respect of high risk customers; and/or
(g) a greater understanding of the personal circumstances of high risk customers, including an awareness of sources of third party information.

(4) Scrutiny of transactions and activity must be undertaken throughout the course of a business relationship to ensure that the transactions and activity being conducted are consistent with the firm's knowledge of the relationship, the customer's business, risk profile, source of funds and source of wealth.

11.4. PEP Relationships

(1) The system of monitoring used by the firm must provide for the ability to identify where a customer, beneficial owner or underlying principal becomes a PEP during the course of the business relationship and whether that person is a foreign, domestic or international organisation PEP.

(2) 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 relationship and the profile of the relationship, including its asset value.

(3) 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 stage. It is therefore essential that ongoing monitoring exists in order to identify changes of status and risk classification.

11.5. High Risk Transactions or Activity

(1) When conducting monitoring, the following are examples of red flags which may indicate high risk transactions or activity:

(a) an unusual transaction in the context of the firm's understanding of the business relationship (e.g. abnormal size or frequency for that customer or peer group, or a transaction or activity involving an unknown third party);
(b) customer funds originating from, or destined for, an unusual location, whether specific to an individual customer, 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; or
(g) an association with a jurisdiction or territory that has significant levels of corruption, or provides funding or support for terrorist activities.

(2) Transactions or activity to or from jurisdictions specified in the Business from Sensitive Sources Notices and Instructions issued by the Commission must be subject to a greater level of caution and scrutiny.

11.6. Real-Time and Post-Event Transaction Monitoring

(1) 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. This is in contrast to post-event monitoring which involves periodic, e.g. monthly, reviews of transactions and activity which have occurred over the preceding period.

(2) Real-time monitoring of activity can be effective at reducing exposure to ML, FT and predicate offences such as bribery and corruption, whereas post-event monitoring may be more effective at identifying patterns of unusual transactions or activities.

(3) 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 is identified and flagged for further examination.

11.7. Automated and Manual Monitoring

(1) A firm's monitoring processes should be appropriate in relation to its size, activities, complexity and 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.

(2) Notwithstanding the method of monitoring used, in accordance with paragraph 11 of Schedule 3 the firm shall adapt the parameters of its processes, in particular the extent and frequency of monitoring, on the basis of materiality and risk.

(3) In determining the appropriate parameters for its monitoring processes, the firm must include as a minimum the nature and level of expected transactions and activity and the assessed risk of the business relationships that are being monitored.

(4) Exception procedures and reports can provide a simple but effective means of monitoring all incoming and outgoing transactions and activity involving:

(a) particular geographical locations;
(b) particular products/services/accounts; or
(c) any transaction or activity that falls outside of predetermined parameters within a given time frame.

(5) Where the firm has a high number of customers or a high level of activities, 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, where the firm operates in an e-commerce environment, where the opportunity for human scrutiny of individual transactions and activity is limited.

(6) The firm must ensure that the parameters of any automated system allow for the generation of alerts for large, complex, unusual or higher risk transactions or activity which must be subject to further investigation.

(7) 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 assessment 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.

(8) The firm should be aware that the use of computerised monitoring systems does not remove the requirement for staff to remain vigilant. It is essential that the firm continues to attach importance to human alertness. Factors such as staff intuition; direct exposure to 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 that customer, cannot be automated.

11.8. Investigation

(1) Where the firm identifies any large, complex, unusual or higher risk transaction or pattern of transactions or other activity, it must undertake an investigation of that transaction or other activity in accordance with paragraph 11.8.(2) of this Handbook below.

(2) As part of its investigation, 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 relationships and the cumulative effects this may have on the risk rating(s) attributed to the customer and/or relationship(s).

(3) The firm must ensure that the investigation of any large, complex, unusual or higher risk transaction or pattern of transactions or other activity is sufficiently documented and that such documentation is retained in a readily accessible manner.

(4) The firm must ensure that procedures exist which require that a SAR is filed with the FCRO in accordance with the requirements of chapter 13 of this Handbook where the circumstances of the transaction or activity appear suspicious in any way.

(5) Following the conclusion of its investigation, the firm should give consideration to whether follow-up action is necessary to refine and amend its policies, procedures and controls in light of the identified transaction or activity. This could include, but is not limited to:

(a) undertaking ECDD where this is considered necessary or where the risk rating of the business relationship has changed as a consequence of the transaction or activity;
(b) considering whether further staff training in the identification of large, complex unusual or higher risk transactions and activity is needed, whether there is a need to refine the monitoring system's parameters, or enhancement of controls for more vulnerable products/services/business units; and/or
(c) applying increased levels of on-going monitoring for particular relationships.

11.9. Ongoing Customer Due Diligence

(1) The requirement to conduct ongoing CDD will ensure that the firm is aware of any changes in the development of the business relationship. The extent of the ongoing CDD measures must be determined on a risk sensitive basis. However the firm must be aware that as the relationship develops, the risks of ML and FT may change.

(2) The Commission would expect ongoing CDD to be conducted on a periodic basis in line with the requirement to review customer risk assessments in accordance with subparagraph 3(4)(b) of Schedule 3, or where a trigger event occurs in the intervening period.

(3) It should be noted that it is not necessary to re-verify or obtain current documentation 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 circumstances, such as a change of address.

(4) In order to reduce the burden on customers in low risk business relationships, trigger events, e.g. 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. Board Oversight

(1) The board, the FCRO and the FCCO should have access to, and familiarise themselves with, the results and output from the firm's monitoring processes. Such output should be regularly reviewed by the board and action taken where concerns or discrepancies are identified.

(2) In some cases the firm may form part of a group which provides a variety of financial services and/or prescribed business, either through a group network or via individual entities. The diversity of such services presents differing challenges in respect of monitoring ML, FT and sanctions risks across the breadth of business. Where the firm undertakes cross-sectorial business, it should have controls and measures in place, including in respect of ongoing

monitoring, which provide for engagement with the varying units and the capability to review or share information for relationships utilising more than one business function or service.

(3) The board should review the appropriateness and effectiveness of the monitoring processes as part of its annual review of the firm's business risk assessment and associated policies procedures and controls. In accordance with paragraph 11 of Schedule 3 this shall include consideration of the extent and frequency of such monitoring, based on materiality and risk as set out in the business risk assessment.

(4) 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 Rule 2.7.(1) of this Handbook.

Chapter 12
UN, EU and Other Sanctions

Contents of this Chapter

Schedule 3 Requirements

The requirements of Schedule 3 to the Law to which the Commission Rules and guidance in this chapter particularly relate are:

- Paragraph 11, which provides for the monitoring of transactions and other activity and for conducting ongoing due diligence.

  Paragraph 11 Hyperlink

- Paragraph 15, which makes provisions in relation to corporate governance and the review of compliance.

  Paragraph 15 Hyperlink

Useful Sources

The following websites provide further information about sanctions, including their nature and scope and details of the various regimes:

- The States of Guernsey:
  https://www.gov.gg/sanctions
- The UN Security Council Sanctions Committee:
  https://www.un.org/sc/suborg/en/scsb
- The Council of the European Union:
  http://eeas.europa.eu/cfsp/sanctions/index_en.htm
- The UK Office for Financial Sanctions Implementation:
  https://www.gov.uk/sanctions-embargoes-and-restrictions
- The US Office of Foreign Assets Control:
  https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx

12.1. Introduction

(1) A sanction is a measure imposed by a government using laws and regulations 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; and/or
(e) suspension from international organisations.

(2) 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. All recent UN and EU sanctions contain information as to their intended aim or purpose.

(3) This chapter outlines the statutory provisions applicable to firms within the Bailiwick concerning UN, EU and other 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. Overview

(1) The two key supranational bodies to determine sanctions measures relevant to the sanctions regime within the Bailiwick are the UN and the EU.

(2) The UN Security Council can take measures to maintain, or restore, international peace or security. Such measures range from economic sanctions to international military action. Each UN member state is then called upon to implement the requirements of a sanctions measure in its own territory.

(3) The EU applies sanctions in pursuit of the specific objectives of the Common Foreign and Security Council as set out in the Treaty of the European Union. EU sanctions are either adopted to ensure compliance with UN sanctions requirements or enacted autonomously by the EU to advance specific EU objectives. EC regulations imposing sanctions apply directly in member states. Further legislation is, however, required in each member state to impose penalties for sanctions breaches under EC regulations.

(4) EC regulations impose restrictive measures in respect of designated persons, that is, persons, groups or entities designated by the UN Sanctions Committee. These designated persons are listed in Annex 1 to EC regulations.

(5) A country may also impose sanctions unilaterally as an extension of its own foreign policy, e.g. the UK via HM Treasury or the US via OFAC.

12.3. The Bailiwick's Sanctions Regime

(1) The Bailiwick has enacted numerous pieces of legislation which implement sanctions measures, many dealing specifically with terrorist financing, the aim of which is to limit the availability of funds and financial services to terrorists and terrorist organisations:

- The Terrorist Asset-Freezing Law
  The Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011

- The Afghanistan (Restrictive Measures) Ordinance, 2011
  The Afghanistan (Restrictive Measures) (Guernsey) Ordinance, 2011
  The Afghanistan (Restrictive Measures) (Alderney) Ordinance, 2011
  The Afghanistan (Restrictive Measures) (Sark) Ordinance, 2011

- The Al-Qaida (Restrictive Measures) Ordinance, 2013
  The Al-Qaida (Restrictive Measures) (Guernsey) Ordinance, 2013
  The Al-Qaida (Restrictive Measures) (Alderney) Ordinance, 2013
  The Al-Qaida (Restrictive Measures) (Sark) Ordinance, 2013

- The Terrorism Law
  The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002

(2) In addition to the sanctions regime implemented by the above enactments, the Bailiwick has passed additional legislation to implement a wide range of country-specific sanctions. 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.

(3) Although the Bailiwick's sanctions regime is based on legislation that broadly mirrors equivalent legislation in the UK, it is completely separate from, and operates independently of, the UK regime.

(4) 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. In addition, the legislative frameworks of some jurisdictions 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.

(5) The firm should be aware, in particular, of sanctions implemented by OFAC. OFAC regulations can be applied to:

(a) US citizens and permanent resident immigrants regardless of where they are located;
(b) persons and entities within the US;
(c) persons and entities trading in US Dollars;
(d) US incorporated entities and their foreign branches;
(e) in the cases of certain sanctions, such as those regarding Cuba and North Korea, all foreign subsidiaries owned or controlled by US companies; and
(f) in certain cases, foreign persons in possession of US origin goods.

12.4. The Bailiwick's Sanctions Regime – Sanctions Committee

(1) The Bailiwick has established a Sanctions Committee to co-ordinate sanction activities, ensure information is distributed publicly and to provide advice on sanctions. The Sanctions Committee reports to the External Relations Group of the States of Guernsey's Policy and Resources Committee and to the Bailiwick's AML/CFT Advisory Committee.

12.5. The Bailiwick's Sanctions Regime – External Relations Group

(1) The External Relations Group is mandated on behalf of the Policy and Resources Committee to:

(a) agree to implement new sanctions measures;
(b) license frozen funds; and
(c) administer notifications and authorities, e.g. those under specific ordinances.

(2) The External Relations Group also works with HM Treasury and the Foreign Commonwealth Office.

12.6. Obligation to Report

(1) Under the Terrorist Asset-Freezing Law, together with the Afghanistan (Restrictive Measures) Ordinance, 2011 and the Al-Qaida (Restrictive Measures) Ordinance, 2013 (collectively "the Restrictive Ordinances"), 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 Restrictive Ordinances. This requirement is in addition to the reporting obligations in the Disclosure Law and the Terrorism Law.

(2) The firm should be aware that the effects of failing to comply with the Terrorist Asset-Freezing Law or the Restrictive Ordinances 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.

12.7. Designated Persons

(1) A designated person means any natural or legal person, group or entity which is:

(a) designated by the Policy and Resources Committee under the Terrorist Asset-Freezing Law;
(b) the subject of a designation under and within the meaning of the UK's Terrorist Asset-Freezing etc. Act 2010; or
(c) included in the list provided for by Article 2(3) of Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism (as amended from time to time).

12.8. Licences

(1) The States of Guernsey's Policy and Resources Committee may grant a licence permitting the release of specified funds which would otherwise be caught by the provisions of the Terrorist Asset-Freezing Law and of the Restrictive Ordinances. No offence is committed in respect of such funds provided that the terms of the licence are complied with.

(2) The Policy and Resources Committee will consider applications for licences under the Terrorist Asset-Freezing Law and the Restrictive Ordinances from any party. Such licences will normally only be issued in respect of funding for necessities such as food, medical treatment and accommodation, but funding for extraordinary expenses will also be considered.

12.9. Policies, Procedures and Controls

(1) The firm must have in place appropriate and effective policies, procedures and controls to identify, in a timely manner, whether a prospective or existing customer or any beneficial owner or underlying principal is the subject of a sanction.

(2) Regardless of the method or system utilised, the firm must ensure that the lists of individuals and legal entities designated by the UN, the EU and the States of Guernsey's Policy and Resources Committee are consulted when identifying whether a customer or prospective customer, beneficial owner or underlying is subject to sanction.

(3) HM Treasury maintain a list which includes all persons whose designation is effective in the Bailiwick (including designations by the EU and UN), other than those persons specifically designated by the Policy and Resources Committee under the Terrorist Asset-Freezing Law who are separately listed by the States of Guernsey. Both lists can be found through the below links:

https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets

http://www.gov.gg/sanctionsmeasures

(4) It should be noted that the UN and EU do not have a notification facility for advising when the lists of designated persons maintained by them are updated. However, HM Treasury (including UN and EU designations) and OFAC both offer facilities for notification by e-mail when a financial sanctions related release is published. Below are links to both facilities:

http://engage.hm-treasury.gov.uk/fin-sanc-subscribe/

https://service.govdelivery.com/accounts/USTREAS/subscriber/new?topic_id=USTREAS_61

(5) In addition to the above, 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 SDNs. Their assets are blocked and US entities are prohibited from dealing with them. The list, and a free OFAC search facility, can be found through the below links:

http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx

http://sdnsearch.ofac.treas.gov

(6) The firm must have in place a system and/or control to detect and block transactions connected with those persons designated by the Bailiwick's sanctions regime.

(7) The transaction monitoring systems and/or controls used should enable the firm to identify:

(a) transactions, both incoming and outgoing, involving designated persons; and
(b) transactions where limited identifying information has been input with the intention of circumventing sanctions monitoring controls (see chapter 14 of this Handbook).

12.10. Customer Screening

(1) In order to comply with Rule 12.9.(2) above, the firm should as a minimum undertake sanctions screening for all new customers, beneficial owners and underlying principals at the time of take-on, during periodic reviews and when there is a trigger event generating a relationship review.

(2) Following changes to the lists of persons designated by the UN or EU, 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 FIS via THEMIS and the Commission through its website.

https://mlro.gov.gg
https://www.gfsc.gg

(3) The firm should have appropriate 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 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.

(4) The firm should maintain an audit trail of the sanctions screening conducted. The audit trail should allow for the firm to demonstrate the dates on which screening checks have been undertaken, the results of those checks and any follow-up action taken.

12.11. Compliance Monitoring Arrangements

(1) 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 Bailiwick sanctions regime.

(2) Testing undertaken should cover the following:

(a) the accuracy of the screening system(s) or method(s) utilised to ensure that designated persons are promptly identified;
(b) the appropriateness of the firm's controls, including the method(s) and frequency of testing;
(c) 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
(d) the action taken by the firm where a sanctions match has been identified to ensure that the proceeds associated with designated persons are appropriately controlled and the necessary reporting undertaken in compliance with applicable regulatory requirements.

(3) 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.

Chapter 13
Reporting Suspicion

Contents of this Chapter

Schedule 3 Requirements

The requirements of Schedule 3 to the Law to which the Commission Rules and guidance in this chapter particularly relate are:

- Paragraph 12, which provides for the reporting and disclosing of suspicion.

  Paragraph 12 Hyperlink

- Paragraph 15, which makes provisions in relation to corporate governance and the review of compliance, including the requirement to appoint an FCCO.

  Paragraph 15 Hyperlink

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 and the Terrorism and Crime (Bailiwick of Guernsey) Regulations, 2007 as amended (together "the Reporting Regulations").

(3) The firm should note that the court will take account of the rules and guidance provided in this Handbook in considering compliance with the disclosure requirements of the Reporting Laws, Reporting Regulations and Schedule 3.

(4) 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.

(5) References in this chapter to any suspicion are references to suspicion of either ML or FT.

(6) References in this chapter to criminal activity are references to all criminal acts that would constitute a predicate offence for ML.

(7) References to terrorist financing are references to the financing of terrorist acts or terrorist organisations, or individual terrorists, even in the absence of a link to a specific terrorist act or acts.

13.2. Definition of Knowledge or Suspicion

(1) Suspicion is a subjective issue. However, it is something less than personal or subjective knowledge but which falls short of proof based on firm evidence. The Reporting Regulations do not define suspicion, though there is a body of UK case law which can assist the firm in determining if there is sufficient knowledge or suspicion to report to the FIS.

(2) 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''.

(3) In the case of Shah v HSBC[2], the UK High Court took the view that there is a very low threshold for suspicion, which does not have to be either reasonable or rational.

(4) The UK courts have therefore defined suspicion as beyond mere speculation, being based on some substance. In this respect the individual filing a SAR must think there is a possibility, more than merely fanciful, that the relevant facts exist and the suspicion must be of a settled nature.

[1] R v Hilda Gondwe Da Silva [2006] 2 Crim App R 35
[2] Shah v HSBC Private Bank (UK) Limited [2012] EWHC 1283

13.3. Obligation to Report

(1) In accordance with the requirements of the Reporting Laws, all suspicious transactions and activity, including attempted transactions and activity, shall be reported regardless of the amount of the transaction.

(2) A suspicion may be based upon:

(a) a transaction or attempted transaction or activity which is inconsistent with a customer's known legitimate business, activities or lifestyle or with the normal business for that type of product/service; or

(b) a belief that the firm has committed an ML and/or FT offence by becoming involved in:
  (i) concealing or transferring the proceeds of crime;
  (ii) assisting another person to retain the proceeds of criminal conduct; or
  (iii) the acquisition, possession or use of the proceeds of criminal conduct; or

(c) information from other sources, including law enforcement agencies, other government bodies, the media, intermediaries, or the customer themselves.

(3) 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.

(4) The board of the firm and all relevant 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.

(5) What may constitute reasonable grounds for knowledge or suspicion will be determined from facts or circumstances from which an honest and reasonable person engaged in a firm would have inferred knowledge or formed the suspicion that another was engaged in ML or FT.

(6) 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, e.g., an out of the ordinary transaction or activity within a business relationship should prompt the firm to conduct enquiries about the transaction or activity.

(7) 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 should be made having due regard to the tipping off provisions.

(8) 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 the CDD or its understanding of a particular transaction or activity or proposed transaction or activity.

13.4. Attempted Transactions

(1) There is no generic definition of an attempted transaction in the Handbook or the relevant enactments. 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. 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.

(2) 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.

(3) 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, e.g. 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 authorities. Depending upon the information received, the firm may form a suspicion of ML and/or FT in which case a disclosure must be submitted to the FIS in accordance with the Disclosure Law or the Terrorism Law.

(4) The FIS 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 FIS.

Financial Investigation Unit - Attempted Transactions

13.5. Potential Red Flags

(1) The following is a non-exhaustive list of possible red flags that the firm should be mindful of when dealing with a customer:

(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 its circumstances;
(c) transactions involving the unexplained movement of funds, either as cash 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 becomes active after a period of dormancy; or
(h) the customer is unable or reluctant to provide details or credible explanations for establishing a business relationship, opening an account or conducting transactions;
(i) the customer holds multiple bank accounts for no apparent commercial or other reason.

(2) The above list is not exhaustive and its content is purely provided as examples of possible red flags. The existence of one or more red flag 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

(1) The firm must establish appropriate and effective policies, procedures and controls in order to facilitate compliance with the reporting requirements of the Reporting Laws and the Reporting Regulations. The policies, procedures and controls must ensure that:

(a) each suspicion is reported to the FCRO 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) the FCRO promptly considers each such internal suspicion report and determines whether it results in there being knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that someone is engaged in ML and/or FT or that certain property represents, or is derived from, the proceeds of criminal conduct or terrorist property;
(c) where the FCRO has determined that an internal suspicion report does result in there being such knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that someone is engaged in ML and/or FT, that the FCRO discloses that suspicion to the FIS; and
(d) where, during the CDD process, the firm knows or suspects that someone is engaged in ML and/or FT a disclosure is made to the FIS under the Reporting Laws.

13.7. Internal Reporting

(1) The firm must have appropriate and effective internal reporting policies, procedures and controls to ensure that:

(a) all employees know to whom within the firm and in what format their suspicions must be reported;
(b) all suspicion reports are considered by the FCRO and where the FCRO makes a decision not to make a disclosure to the FIS, the reasons for the decision not to disclose are documented and retained;
(c) enquiries made in respect of disclosures must be recorded and documented; and
(d) once a disclosure has been made to the FIS, the FCRO immediately informs the FIS where subsequent relevant information or documentation is received.

(2) The FCRO should consider whether to include within the firm's procedures the provision of an acknowledgment to evidence the submission of a SAR. Such an acknowledgement provides confirmation to the submitter that his statutory obligations have been fulfilled.

13.8. Form and Manner of Disclosing to the FIS

(1) In accordance with the requirements of the Reporting Laws, suspicion of ML (including drug ML) must be disclosed under the provisions of the Disclosure Law and suspicions relating to FT must be disclosed under the Terrorism Law.

(2) The Reporting Laws require that information contained in internal reports made to an FCRO is disclosed to the FIS where the FCRO knows or suspects or has reasonable grounds for knowing or suspecting, as a result of the internal report, that a person is engaged in ML and/or FT.

(3) The Reporting Regulations provide that disclosures to the FIS are to be made through the online reporting facility THEMIS:

https://mlro.gov.gg

(4) Prior to making a disclosure to the FIS, the firm should consider all available information in respect of the business relationship or occasional transaction. Notwithstanding this consideration, disclosures to the FIS should be made promptly following a determination by the FCRO that a disclosure is appropriate.

(5) Where the FCRO considers that a disclosure should be made urgently, e.g. where the customer's product is already part of a current investigation, initial notification to the FIS may be made by telephone.

Financial Investigation Unit – Contact Details

13.9. Information to Provide with a Disclosure

(1) The firm must provide the FIS with a full account of circumstances and grounds (suspected underlying criminality) for suspicion. In providing such detail the firm must include as much information and documentation (e.g. CDD documentation, statements, contract notes, correspondence, minutes, transcripts, etc.) as possible to demonstrate why suspicion has been raised and to enable the FIS to fully understand the purpose and intended nature of the business relationship or occasional transaction.

(2) The firm should examine all connected accounts and/or relationships. Research of connected accounts or relationships should not delay making a disclosure.

(3) 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 both 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 and/or FT, and any fact or matter upon which such knowledge, suspicion or reasonable grounds for suspicion is based.

(4) Firms are also required to provide the FIS with the reasons for suspicion. Firms must clearly define the grounds for suspicion and any specific indicators or suspected criminality within the main body of the report. Firms may have multiple grounds i.e. ML and tax evasion or bribery and corruption and fraud.

(5) 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.

13.10. Group Reporting

(1) It is for each firm or group to consider whether, in addition to any disclosure made in the Bailiwick, the FCRO should report suspicions within the firm or group, e.g. 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 FIS.

(2) 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, e.g. if the subject of the disclosure is subject to ongoing investigation by the FIS. In this respect, consideration should be given by the firm to anonymising disclosures prior to onward reporting.

13.11. The Response of the FIS

(1) Disclosures made through THEMIS are acknowledged immediately.

(2) If the disclosure does not refer to a specific transaction or activity that could constitute an ML or FT offence, the response from the FIS will simply acknowledge receipt of the disclosure.

(3) If the disclosure does include reference to a specific transaction or activity that has led to the suspicion and ultimately a disclosure, the firm should indicate whether or not it intends to carry out the transaction or activity, and if so request consent from the FIS to continue with the particular transaction or activity. The FCRO should exhaust all avenues at his disposal to either negate or confirm whether or not there is a suspicion before seeking FIS consent. Upon receipt of such a request the FIS will consider whether or not it may give consent under the relevant provisions. The FIS will, except in exceptional circumstances, advise in writing the nature of its decision regarding the request within seven days of receipt of the disclosure. In urgent matters, consent may be given orally by the FIS, but will be followed by written confirmation.

(4) Access to disclosures will be restricted to appropriate authorities and any information provided by the FIS 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.

(5) In addition, the FIS 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. Tipping Off

(1) The Reporting Laws provide that it is a criminal offence for a person, who knows or suspects that a SAR to an FCRO or a disclosure to the FIS has been or will be made, or any information or other matter concerning a SAR or disclosure has been or will be communicated to an FCRO or the FIS, 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.

(2) 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.

(3) 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.

(4) If the firm identifies open source information on the customer, e.g. a media article that the customer is or has been subject to criminal proceedings, this should not give rise to tipping off. However, the firm should consider reporting the matter to the FIS by way of a disclosure.

(5) HM Procureur has issued a paper entitled Guidance on Prosecution for Tipping Off which provides for disclosures made to members of the same organisation or linked organisations to discharge their AML and CFT responsibilities.

Guidance on Prosecution for Tipping Off

(6) The firm's policies, procedures and controls must enable an FCRO to consider whether it is appropriate to disclose a suspicion 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 this process. Such procedures must also provide for the FCRO 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.

(7) There will be occasions where it is feasible for the firm to agree a joint strategy with the FIS, but the FIS will not seek to influence what is ultimately a decision for the firm and the online reporting facility cannot be used for this purpose.

13.13. Terminating a Business Relationship

(1) Whether or not to terminate a business relationship is a commercial decision, except where required by law, e.g. where the firm cannot obtain the required CDD information (see chapter 4 of this Handbook and paragraph 9 of Schedule 3).

(2) Where the firm takes the decision to terminate a business relationship after it has made a disclosure or requested FIS consent and is concerned that, in doing so, it may prejudice an investigation or contravene the tipping off rules, it must engage with the FIS accordingly. The decision to terminate a business relationship, however, remains with the firm.

13.14. FIS Requests for Additional Information

(1) Under Regulation 2 of the Reporting Regulations, the FIS 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.

(2) An amendment to the Reporting Regulations came into force on 7 August 2014 providing that, if a disclosure has been made, the FIS can request information relating to that disclosure from a third party if it is satisfied that there are reasonable grounds to believe that the third party possesses relevant information and that there are reasonable grounds to believe that the information is necessary to the FIS for the proper discharge of its functions.

(3) 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.

(4) A police officer may, by notice in writing served upon a third party, require that third party to provide the 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.

(5) Ordinarily the information requested under Regulation 2 or Regulation 2A of the Reporting Regulations must be provided within seven days, though the FIS 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.

(6) 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 FIS 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 in the specified time frame is a criminal offence.

13.15. Management Information

(1) The receipt of adequate and appropriate management information is beneficial in helping to ensure that the board of the firm can discharge its responsibilities fully under paragraph 15(1)(a) of Schedule 3.

(2) The management information provided to the board should include, as a minimum:

(a) the number of internal reports;
(b) the level of onward reporting;
(c) an indication of the length of time taken in deciding whether or not to externalise an internal suspicion report; and
(d) the nature of disclosures.

13.16. Record Keeping

(1) 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 which are suspicious from those which are legitimate, it will be necessary to carefully consider all future transactions or activities and the nature of the continuing relationship, and to implement an appropriate risk-based strategy.

(2) It should be borne in mind that suspicion of ML or FT could relate to assets whether they directly or indirectly relate to criminal conduct.

(3) In accordance with Rule 16.6.(2) of this Handbook, in addition to the record keeping requirements in respect of individual SARs and disclosures, a register must also be maintained noting all SARs and disclosures to allow for the FCRO to maintain oversight of matters. This will assist in, amongst other things, identifying trends in SARs and disclosures and vulnerabilities across the firm's customer base.

13.17. Legal Professional Privilege

(1) Pursuant to section 3(6)(d) of the Disclosure Law, a person does not commit an offence for failing to report a suspicion of ML or FT where he is a professional legal adviser and the information or other matter came to him in privileged circumstances. It should be noted, however, that information held with the intention of furthering a criminal purpose would not be subject to LPP.

(2) 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 legal adviser, without fear of later disclosure to his prejudice. It is an absolute right and cannot be overridden by any other interest.

(3) LPP belongs to the customer, not the legal professional, and may only be waived by the customer.

(4) LPP does not 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 – legal advice privilege or litigation privilege:

(a) legal advice privilege – protects confidential communications between lawyers acting in their legal professional capacity and their customers, made for the dominant purpose of seeking or giving legal advice; or
(b) litigation privilege – applies where there is 'a real likelihood' of litigation or litigation is actually underway and which protects confidential communications between lawyers and customers or between lawyers and third parties and documents created by, or on behalf of, a lawyer or his customer.

(5) 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.

(6) LPP protects advice given by a lawyer to a customer on avoiding committing a crime or warning them that proposed actions could attract prosecution. LPP does not 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 lawyer is aware that he is being used for that purpose.

(7) 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 lawyer/communication to be made with that purpose (e.g. where the innocent customer is being used by a third party).

(8) If the firm knows the transaction or activity being worked on is a principal offence, the firm risks committing an offence. Also, communications relating to the transaction or activity are not privileged and can be disclosed.

(9) If the firm merely suspects a transaction or activity might constitute an ML and/or FT 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 non-disclosable.

13.18. THEMIS Notices

(1) THEMIS has the facility to provide firms with notices which are sent via a generic email address to individual users. These notices are a mechanism through which the FIS provides information to all THEMIS users or to specific 'targeted' distribution groups or firms, dependent upon the information or guidance that is being issued.

(2) Notices sent via THEMIS include updates on changes to the legislative framework, news of forthcoming presentations or seminars and updates in respect of EU, UN and other sanctions related updates. In addition to generic updates, the FIS may specifically 'target' certain distribution groups or firms in respect of notification that a certain entity or group of entities is under investigation by the FIS or other law enforcement agencies. In this respect, THEMIS is the mechanism by which specific 'targeted' notices will be distributed to FCROs.

(3) The FCRO should refer to the THEMIS portal regularly and also whenever a notification is issued by the FIS. Where targeted notices are issued, the firm should establish if it maintains a business relationship with the entities listed on the notice or if there is information which may assist the FIS. The firm should consider if this approach (by law enforcement) is sufficient grounds for suspicion to report a SAR to the FIS in accordance with section 13.3. of this Handbook. It should be noted that the FIS have the facility to monitor whether notices have been received and/or read by the recipient.

Chapter 14
Wire Transfers

Contents of this Chapter

Legislation

(1) The requirements of Bailiwick legislation to which the Commission Rules and guidance in this chapter particularly relate are:

- The Transfer of Funds Ordinance, 2017
  The Transfer of Funds (Guernsey) Ordinance, 2017
  The Transfer of Funds (Alderney) Ordinance, 2017
  The Transfer of Funds (Sark) Ordinance, 2017

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 [*TBC*] 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 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 must 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 the 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 standard 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 and FT and to facilitate the effective implementation of restrictive measures against persons and entities designated under UN and EU 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 FIS.

(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 must 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. PSPs must also 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 EU Regulation also introduce increased reporting obligations upon PSPs to identify breaches and areas of non-compliance which must be reported to the Commission. The Transfer of Funds Ordinance prescribes the manner in which such reports must 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 section 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 ESA 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.

ESA Joint Guidelines under Article 25 of Regulation (EU) 2015/847 (in draft)

14.2. Scope

(1) 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.

(2) 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 14.2.(4) below;
(b) transfers of funds carried out using a payment card, electronic money instrument or a mobile phone, or any other digital or 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.

(3) It should be noted that the exemption set out in paragraph 14.2.(2)(b) 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.

(4) 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, that is to say, 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, information technology (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;

(o) 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 as listed in the Annex.

14.3. Outgoing Transfers – Obligations upon the PSP of the Payer

14.3.1. Transfers for Non-Account Holders

(1) In accordance with Article 4 of the EU Regulation, where a transfer of funds is not made from or to an account the PSP must obtain customer identification information on the payer and payee, record that information and verify the customer information on the payer.

(2) Where all of the PSPs involved in the transfer are established in the British Islands and the transfer is in excess of EUR 1,000 in a single transaction or in a linked series of transactions which together exceed EUR 1,000, the transfer must, 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, e.g. the name and address of the payer, is requested by the PSP of the payee or the Intermediary PSP, such information must be provided within three working days of the receipt of a request for such information.

(3) Where a transfer is carried out within the British Islands which is at or below the EUR 1,000 threshold, the customer identification information on the payer and the payee must 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.

(4) 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.

(5) 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 and FT.

(6) 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.

(7) 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

(1) In accordance with Article 4 of the EU Regulation, where a PSP is seeking to make a transfer from an account, the PSP must:

(a) obtain customer identification information on the payer, verify that information, and record and retain that information;
(b) have undertaken customer 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.

(2) 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, e.g. the name and address of the payer, is requested by the PSP of the payee or the Intermediary PSP, such information must be provided by the PSP within three working days of the receipt of a request for such information.

(3) Where a transfer is carried out within the British Islands which is at or below the EUR 1,000 threshold, the customer identification information on the payer and the payee must 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.

(4) 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 and FT.

(5) 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.

(6) Where the transfer is being made to a PSP in any other country or territory, the transfer must 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).

(7) In the case of a payer that is a company, the transfer must include the address at which the company's business is conducted. In the case of a payer that is a trustee, a transfer must be accompanied by the address of the trustee.

(8) Where the payer is a foreign incorporated company administered in the Bailiwick, the address referred to in Rule 14.3.2.(7) would be that of its administrator.

(9) 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.

14.4. Detection of Missing or Incomplete Information

(1) Under Article 4 of the EU Regulation the PSP must ensure that no transfer is executed before ensuring that the transfer includes the required customer identification information on the payer and the payee.

14.5. Batch Files – Transfers Inside or Outside the British Islands

(1) In accordance with Article 6 of the EU Regulation, batch files from a single payer to multiple payees must carry the information identified in section 14.3.1.(4) of this Handbook for the payer and that information must 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).

(2) Where the transfer is at or below 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.

(3) The information requirements of paragraphs 14.3.1.(2), 14.3.2.(2), 14.5.(2) 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.

14.6. Incoming Transfer – Obligations upon the PSP of the Payee

(1) In accordance with Article 7 of the EU Regulation the PSP of the payee must obtain customer identification information on the payee, verify that information and record and retain that information, or to have undertaken customer CDD procedures and retained records in connection with the opening of that account in accordance with Schedule 3 and the Commission Rules.

(2) 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 and FT.

(3) 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 14.7.(4).

14.7. Detection of Missing or Incomplete Information

(1) 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, e.g. by undertaking sample testing to identify fields containing incomplete information on the payer and payee; and where information is incomplete, take specified action.

(2) SWIFT payments on which mandatory information fields are not completed will fail anyway 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 will 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, e.g. BACS.

(3) Under Article 7 of the EU Regulation a PSP of a payee must 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.

(4) 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.

(5) A PSP's policies, procedures and controls should:

(a) take into account the ML and FT 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 staff should do where required information is missing or incomplete.

(6) The level of monitoring should be appropriate to the risk of the PSP being used in connection with ML and FT, 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 FATF Recommendations 10 (CDD); 11 (record-keeping) and 19 (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 it operates.

(7) 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.

(8) Under Article 8 of the EU Regulation a PSP must implement effective risk-based polices, 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.

(9) 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.

(10) 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).

14.8. Failure to Supply Information

(1) 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.

(2) 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.

(3) 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 Recommendations 10 (CDD), 11 (record-keeping) and 19 (wire transfers).

(4) 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.

(5) 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.

(6) 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.

(7) 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.

14.9. Obligations upon an Intermediary PSP

(1) In accordance with Article 10 of the EU Regulation intermediary PSPs (e.g. those acting as agents for other PSPs or who provide correspondent banking facilities) must, 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.

(2) Under Article 11 of the EU Regulation an intermediary PSP must 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.

(3) Under Article 12 of the EU Regulation an intermediary PSP must 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 of if the information fields have been incorrectly filled in.

(4) Article 12 of the EU Regulations 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.

(5) 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.

(6) 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 had been identified through mutual evaluations or other assessments by the FATF as insufficiently applying Recommendations 10 (CDD), 11 (record keeping) and 16 (wire transfers).

(7) 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.

(8) 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.

(9) 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.

14.10. Reporting

(1) 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 FIS;
(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 14.8.(5) and 14.9.(7) above) to the Commission.

14.10.1. Reporting Suspicions

(1) 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 FIS in accordance with Part I of the Disclosure Law and Part II of the Terrorism Law.

(2) 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 and/or FT, 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.

Reporting Suspicion

(3) Staff members 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.

Employee Screening and Training

14.10.2. Reporting Breaches

(1) Under Article 4 of the Transfer of Funds Ordinance a PSP must notify the Commission of breaches of the EU Regulation and the Transfer of Funds Ordinance.

(2) The Commission must set out mechanisms to encourage reporting and ensure that there are appropriate anonymous, independent and secure channels within a PSP for an employee to report breaches.

(3) This reporting requirement applies specifically to breaches of the EU Regulation and the Transfer of Funds Ordinance.

(4) 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 section and any serious breaches of the PSP's policies, procedures and controls in respect of transfers of funds.

(5) Notifications to the Commission should be made promptly and contain the following information:

(a) the specific provision in the EU Regulation, 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.

(6) 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 14.10.2.(5) and the steps it is considering taking under (d).

(7) A PSP must establish policies and procedures for the internal reporting by staff of breaches of the EU Regulation or 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 staff who report breaches committed within the PSP.

14.11. Data Protection

(1) In order to ensure that information provided under the Transfer of Funds Ordinance is also processed in line with the Data Protection (Bailiwick of Guernsey) Law, 2001, it may be advisable for a PSP to ensure that its terms and conditions of business include reference to the information that it may provide under the requirements set out in Article 4 of the Transfer of Funds Ordinance.

14.12. Record Keeping

(1) 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.

(2) Except where the relevant derogations from the EU Regulation apply, the PSP of the payer must 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.

(3) Except where the relevant derogations from the EU Regulations apply, the PSP of the payee must 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

Schedule 3 Requirements

The requirements of Schedule 3 to the Law to which the Commission Rules and guidance in this chapter particularly relate are:

- Paragraph 13, which provides for procedures to be undertaken by a specified business when hiring employees and for the requirements of training relevant employees.

  Paragraph 13 Hyperlink

- Paragraph 15, which makes provisions in relation to corporate governance and the review of compliance.

  Paragraph 15 Hyperlink

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 members of staff who are alert to the potential risks of ML and FT 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

(1) The board must be aware of the obligations of the firm in relation to staff screening and training.

(2) The firm must establish and maintain procedures to monitor and test, on an ongoing basis, the effectiveness of the firm's training policies and procedures. The firm must ensure that the training provided to employees is comprehensive and ongoing and that employees are aware of ML and FT and their obligations in relation to it.

(3) Further information on the monitoring and testing of the firm's training policies and procedures and the content of training can be found within chapter 2 of this Handbook.

Corporate Governance – Board Oversight of Compliance

(4) With regard to the monitoring and testing of employee awareness of ML and FT, the firm may consider it appropriate to incorporate an exam or similar form of assessment into its on-going training programme, either as part of the periodic training provided to employees or during the intervening period between training.

(5) Regardless of the methods utilised, the board should ensure that it is provided with adequate information on a sufficiently regular basis in order satisfy itself that the firm's employees are suitably trained to fulfil their personal and corporate responsibilities.

(6) Where the firm outsources its FCRO and/or FCCO functions to a third party service provider, it should also consider the content of chapter 2 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.

Corporate Governance – Outsourcing

15.3. Screening Requirements

(1) 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 taken against the employee or action taken by a professional body;
(c) obtaining and confirming details of any criminal convictions, including the provision of a check of their criminal record (subject to the Rehabilitation of Offenders (Bailiwick of Guernsey) Law, 2002); and
(d) obtaining and confirming details of employment history, qualifications and professional memberships.

(2) The firm must ensure that its consideration under Rule 15.3.(1) above, together with the results of any checks undertaken, are documented and retained.

(3) 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 EU to ensure that a prospective employee does not have suspected or known involvement in terrorist activity.

15.4. Relevant Employees

(1) The requirements of Schedule 3 concerning training apply to employees whose duties relate to actual specified business activities, including board members and senior management (hereafter referred to collectively as "relevant employees") and not necessarily to all employees.

(2) 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 transactions;
(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 he 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. Other Employees

(1) There may be some employees who, by virtue of their function, fall outside of the definition of a relevant employee, e.g. 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.

(2) 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, will need to have a basic understanding of ML and FT, together with an awareness of the firm's internal reporting procedures and the identity of the FCRO and NO(s).

(3) 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 a SAR; and

(b) require the employee to acknowledge that he understands the firm's written explanation and procedures for making SARs.

15.6. Method of Training

(1) While there is no single or definitive way to conduct employee training, the critical requirement is that training must be adequate and relevant to those being trained and that the content of the training should reflect good practice.

(2) The guiding principle of all financial crime training should be to encourage 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 and FT.

(3) The precise approach adopted will depend on 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 people to be trained.

(4) Training should highlight to employees the importance of the contribution that they can individually make to the prevention and detection of ML and FT. 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

(1) The firm must provide the appropriate level of AML and CFT induction training or a written explanation to all new employees before they become actively involved in the day-to-day operations of the firm.

(2) 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 and CFT 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.

(3) The firm must provide AML and CFT 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 or services.

15.8. Content of Training

(1) 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 and CFT; and
(d) ensure relevant employees are fully aware of all applicable legislative requirements.

(2) The firm must ensure that the ongoing training provided to relevant employees in accordance with Schedule 3 and this Handbook as a minimum covers:

(a) the requirements for the internal and external reporting 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 FCRO and NO(s);
(d) dealing with business relationships or occasional transactions subject to an internal SAR, including managing the risks of tipping off and handling questions from customers;
(e) those aspects of the firm's business deemed to pose the greatest ML and FT 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) the business risk assessments and risk appetite of the firm and the implications of these on the day-to-day functions of relevant employees, e.g. in relation to new business;
(g) new developments in ML and FT, including information on current techniques, methods, trends and typologies;
(h) the firm's policies, procedures and controls surrounding risk and risk awareness, particularly in relation to CDD and the management of high risk and existing relationships;
(i) the identification and examination of unusual transactions or activity outside of that expected for a customer;
(j) the nature of terrorism funding and terrorist activity in order that staff are alert to customer transactions or activities that might be terrorist-related;
(k) the vulnerabilities of the firm to financial misuse by PEPs, including the effective determination of PEPs and the understanding, assessing and handling of the potential risks associated with PEPs; and
(l) UN, EU and other sanctions and the firm's controls to identify and handle natural persons, legal persons and other entities subject to sanction.

15.9. The Board and Senior Management

(1) The board and senior management are responsible for the effectiveness and appropriateness of the firm's policies, procedures and controls to counter ML and FT. 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.

(2) 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 and FT business risk assessments and the formulation of a risk appetite, together 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 Financial Crime Reporting Officer and Nominated Officer(s)

(1) The FCRO and NO(s) are responsible for, amongst other things, the handling of SARs and disclosures. In accordance with paragraph 13(3) of Schedule 3, the FCRO and NO(s) must be identified as relevant employees to whom additional training must be given.

(2) The additional training provided to the FCRO and NO(s) must include, at a minimum:

(a) the handling of SARs and the reporting of disclosures;
(b) 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;
(c) liaising with the Commission and law enforcement agencies; and
(d) the management of the risk of tipping off.

15.11. The Financial Crime Compliance Officer

(1) The FCCO is responsible for monitoring and testing the effectiveness and appropriateness of the firm's policies, procedures and controls to counter ML and FT. In accordance with paragraph 13(3) of Schedule 3, the FCCO must be identified as a relevant employee to whom additional training must be given.

(2) The training provided to the FCCO 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 and FT.

Chapter 16
Record Keeping

Contents of this Chapter

Schedule 3 Requirements

The requirements of Schedule 3 to the Law to which the Commission Rules and guidance in this chapter particularly relate are:

- Paragraph 14, which provides for the record keeping requirements of a specified business.

  Paragraph 14 Hyperlink

- Paragraph 15, which makes provisions in relation to corporate governance and the review of compliance, including the requirement to appoint an FCCO.

  Paragraph 15 Hyperlink

16.1. Introduction

(1) This chapter outlines the Commission Rules in relation to record keeping and provides guidance to the firm for the purpose of countering the threat of ML and FT.

(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 and FT and confiscation of criminal property may not be possible. Likewise, if the funds used to finance terrorist activity cannot be traced back through the financial system, then the sources and destinations of terrorist 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 the statutory obligations and regulatory requirements.

16.2. General and Legal Requirements

(1) To ensure that the record keeping requirements of Schedule 3 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.

(2) The existence of sound policies, procedures and controls allow for records to be available on a timely basis, i.e. promptly to domestic competent authorities pursuant to Schedule 3 or the Relevant Enactments and to auditors.

16.3. Customer Records

(1) In order to meet the requirements of paragraph 14(2) of Schedule 3 in relation to transaction documents, 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 underlying principals (e.g. copies of records of official identification documents such as passports, identity cards, driving licences or similar);
- (b) copies of any customer risk assessments carried out in accordance with paragraph 3(4) of Schedule 3 and chapter 3 of the 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 (e.g. 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.

(2) The minimum retention period for CDD documentation and information is five years starting from the date that the business relationship ceased or the occasional transaction was completed.

16.4. Transactions

(1) 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 enable the reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

(2) The firm must ensure that in order to meet the record keeping requirements for transactions, documentation is maintained which must include:

(a) the name and address of the customer, beneficial owner and underlying principal;
(b) for monetary transactions, the currency and amount of the transactions;
(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.

(3) Records relating to unusual and complex transactions and high risk transactions must include the firm's own reviews of such transactions.

(4) The minimum retention period for transaction documentation is five years commencing from the date that the transaction and any related transaction were completed.

16.5. Wire Transfers

(1) 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.

Wire Transfers – Record Keeping

16.6. Internal and External SARs and Disclosures

(1) In order to meet the requirements of paragraph 14(5)(a) of Schedule 3 to keep records of SARs made to the FCRO, the firm must keep:

(a) the SAR and any supporting documentation;
(b) records of actions taken under the internal and external reporting requirements;
(c) evidence of the enquiries made in relation to that SAR;
(d) where the FCRO (or a NO) has considered information or other material concerning possible ML and FT, but has not made a disclosure to the FIS, a record of the other material that was considered and the reason for the decision; and
(e) where a disclosure has been made to the FIS, evidence of the FCRO's (or NO's) decision and copies of all relevant information passed to the FIS.

(2) In addition to the above, the firm must maintain a register including both SARs and disclosures made to the FIS. The register must include the following as a minimum:

(a) the date the SAR was received by the FCRO (or a NO);
(b) the name of the person submitting the SAR;
(c) the date of the disclosure to the FIS (if applicable);
(d) the name of the person who submitted the disclosure to the FIS (if applicable);
(e) the value of the transaction or activity subject to the SAR/disclosure (where available);
(f) a reference by which supporting evidence is identifiable; and
(g) the date(s) of any update(s) (additional information) that have been submitted to the FIS.

(3) The minimum record retention period for SARs and disclosures is five years starting from the date that the related business relationship ceased or occasional transaction was completed.

16.7. Training

(1) In order to meet the requirements of paragraph 14(5)(b) of Schedule 3 to keep records of AML and CFT training undertaken, the firm must record the following:

(a) the dates training was provided;
(b) the nature of the training; and
(c) the names of the employees who received training.

(2) The minimum retention period for training documentation is five years starting from the date the training was carried out.

16.8. Compliance Monitoring

(1) In order to meet the requirement to keep records of documents prepared in connection with the requirement of the board to review compliance and of its compliance review policy and other policies, procedures and controls relating to compliance, the firm must retain:

(a) reports by the FCRO to the board and senior management;
(b) records or minutes of consideration of those reports and of any action taken as a consequence;
(c) copies of any business risk assessments prepared in accordance with paragraph 3(1) of Schedule 3; and
(d) any records made within the firm or by other parties in respect of compliance with Schedule 3 and this Handbook.

(2) The minimum retention period for any minutes or other documents prepared in relation to the board's review of its compliance with Schedule 3 and this Handbook is five years starting from the date they were finalised, or they are superseded by later minutes or other documents prepared under Schedule 3 or this Handbook, whichever occurs later.

(3) The minimum retention period for the policies, procedures and controls established and maintained by a firm pursuant to Schedule 3 and this Handbook is five years starting from the date they ceased to be operative.

16.9. Closure or Transfer of Business

(1) Where the firm terminates activities or disposes of a business or a block of business relationships, e.g. by way of asset sale to another firm, the person taking on that business must ensure that the record keeping requirements of Schedule 3 are complied with in respect of such business.

16.10. Ready Retrieval

(1) Regardless of the manner in which information and documentation is stored, the overriding factor is that records are readily retrievable and can be accessed as required, without delay.

(2) Periodically the firm must review the ease of retrieval of, and condition of, paper and electronically retrievable records.

(3) Schedule 3 requires that documents are to be made available promptly to domestic competent authorities where so requested under Schedule 3 or another of the Relevant Enactments. The firm must therefore consider the implications for meeting this requirement 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.

(4) Where the FIS or another domestic competent authority requires sight of records, 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 FIS or other domestic competent authority as possible.

(5) The firm must not enter into outsourcing arrangements or place reliance on third parties to retain records where access to records is likely to be restricted as this would be in breach of Schedule 3 which requires records to be readily retrievable.

16.11. Manner of Storage

(1) 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.

(2) 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).

(3) The use of technology to collect and/or store data and documents does not alter the obligations and requirements described in this Handbook.

(4) The firm should include in its technology risk assessment, an evaluation of the policy for the retention of documents in electronic format to ensure they do not incur legal evidential difficulties, e.g. in civil court proceedings.

Chapter 17
Transitional Provisions

Contents of this Chapter

Schedule 3 Requirements

The requirements of Schedule 3 to the Law to which the Commission Rules and guidance in this chapter particularly relate are:

- Paragraph 3, which provides for a specified business to identify and assess the risks of ML and FT, both in respect of its business as a whole and its individual business relationships or occasional transactions. The paragraph also provides for a firm to ensure that its policies, procedures and controls are effective and appropriate to the assessed risk.

  Paragraph 3 Hyperlink

- Paragraph 4, which provides for the required CDD measures, when and to whom they should be applied.

  Paragraph 4 Hyperlink

- Paragraph 5, which provides for ACDD and ECDD measures in respect of business relationships and occasional transactions where the circumstances necessitate additional measures or the business relationship or occasional transaction has been assessed as high risk.

  Paragraph 5 Hyperlink

- Paragraph 6, which provides for SCDD measures to be applied to business relationships or occasional transactions which have been identified as being low risk or in accordance with the NRA.

  Paragraph 6 Hyperlink

- Paragraph 8, which makes provisions in relation to anonymous accounts and shell banks.

  Paragraph 8 Hyperlink

- Paragraph 15, which makes provisions in relation to corporate governance and the review of compliance, including the requirement to appoint an FCCO.

  Paragraph 15 Hyperlink

17.1. Introduction

(1) This chapter details the measures to be implemented by the firm in order to transition existing compliance arrangements to the requirements of Schedule 3 and the Commission Rules, together with the deadlines by which such controls are required.

(2) In accordance with paragraph 5(1) of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) Ordinance, 2017, the requirements of Schedule 3 come in to force on 31 December 2017. 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 as part of its regular monitoring and ongoing CDD arrangements.

(3) 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 have regard to the content of Schedule 3 and this Handbook when considering the full scope of the changes required to be made.

17.2. Business Risk Assessments

(1) 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 during the ML and FT risk assessments will enable the firm to assess the appropriate controls required to mitigate and manage any risks arising.

(2) In order to meet the requirements of paragraph 3 of Schedule 3 and chapter 3 of this Handbook, the firm must review its business risk assessments to ensure that they:

- (a) contain suitable, sufficient and separate assessments of the ML and FT risks posed to the firm's business;
- (b) incorporate, or makes reference to, any other pertinent assessments conducted in accordance with the requirements of this Handbook, e.g. in respect of the use of technology; and
- (c) take account of the conclusions of the Bailiwick's NRA.

(3) The board of the firm is responsible for ensuring that a review of the business risk assessments is conducted and documented and must approve the revised document(s) by 31 December 2017 or as soon as reasonably practicable thereafter.

(4) For the purposes of Commission Rules 17.2.(2) and 17.2.(3), it is the Commission's expectation that the firm will have revised its business risk assessments and that the revised document(s) will have been approved by the board of the firm by no later than 28 February 2018.

17.3. Policies, Procedures and Controls

(1) In accordance with a risk-based approach, the policies, procedures and controls devised and utilised by the firm are driven by its assessment of the risks of ML and FT. In this regard, the policies, procedures and controls of the firm should be reviewed in parallel with the business risk assessment to ensure that any changes in the perceived threats and vulnerabilities of the firm are mitigated and managed by the controls established.

(2) The firm must review the policies, procedures and controls established by the firm to ensure that they remain appropriate and effective, in light of both revisions to the business risk assessments of the firm in accordance with Rule 17.2.(2) above and any new or altered requirements within Schedule 3 and the Commission Rules.

(3) The board of the firm must ensure that a review is conducted, and must approve the revised policies, procedures and controls, by 31 December 2017.

(4) In addition to reviewing its high level procedures, the firm should also review its controls to ensure 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 customer risk-rating process are taken into account, together with any changes to the due diligence required for various types of customer;
(b) employee training arrangements: to ensure that any new or amended risks identified as part of the risk assessment process are communicated to staff, together with the firm's risk appetite; and
(c) any automated screening tools used to flag PEPs: to ensure that domestic and international organisation PEPs are flagged as appropriate.

17.4. Financial Crime Reporting Officer

(1) In accordance with paragraph 12(a) of Schedule 3, the firm shall appoint an FCRO to be responsible for managing disclosures under the Reporting Laws. This job was previously undertaken by the Money Laundering Reporting Officer, a position whose functions have now been replaced by the FCRO and FCCO roles. Further information on the FCRO can be found in chapter 2 of this Handbook.

Corporate Governance – Financial Crime Reporting Officer

(2) The board of the firm must ensure that a suitable FCRO is appointed by 31 December 2017 and that notification has been made to the Commission by 14 January 2018 confirming the name and title of the natural person who will hold the position of FCRO and confirming the resignation of the current Money Laundering Reporting Officer.

(3) For the avoidance of doubt, the natural person who previously held the role of Money Laundering Reporting Officer can be appointed as the FCRO; however the above notification is still required.

(4) Notification of the appointment of the FCRO and the resignation of the Money Laundering Reporting Officer should be made via the Commission's Online PQ Portal.

https://online.gfsc.gg

17.5. Financial Crime Compliance Officer

(1) In accordance with paragraph 15(1)(a) of Schedule 3, the firm shall appoint a person of at least management level as the FCCO and provide the name and title of that person to the Commission. Further information on the role of the FCCO, including the requirements in respect of the individual appointed, can be found in chapter 2 of this Handbook.

Corporate Governance – Financial Crime Compliance Officer

(2) The board of the firm must ensure that a suitable FCCO is appointed by 31 December 2017 and that notification has been made to the Commission by 14 January 2018 confirming the name and title of the natural person who will hold the position of FCCO.

(3) For the purpose of paragraph 15 of Schedule 3, notification of the appointment of the FCCO shall be made as soon as reasonably practicable and in any case within 14 days starting from the date of that person's appointment. Notification should be made via the Commission's Online PQ Portal.

https://online.gfsc.gg

17.6. Existing Customers

(1) In order to meet the requirements of paragraph 8(1)(b) of Schedule 3, the firm shall ensure that all business relationships are maintained in a manner which facilitates the meeting of the requirements of Schedule 3.

(2) The firm should apply the risk assessment and CDD requirements of Schedule 3 and this Handbook to existing customers on a risk-based approach. This allows 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.

(3) The review of risk assessments and CDD should be conducted at appropriate times, e.g. depending upon the risk rating of a customer or changes to the circumstances of a customer, taking into account whether and when any CDD measures have previously been undertaken and the adequacy of the data obtained. Any reviews undertaken on existing customers should be viewed as an opportunity to consider and build upon the firm's understanding of the customer's profile and circumstances.

(4) Notwithstanding the above, the board must ensure that all customers rated high risk as at the time of Schedule 3 coming in to force are subject to review by 31 December 2018, with all remaining customers reviewed by 31 December 2019.

(5) In complying with paragraph 8 of Schedule 3, as part of the reviews conducted by the firm in accordance with Rule 17.6.(4) above, the firm must take all steps deemed necessary to ensure that risk assessments are conducted and appropriate CDD is held, including ACDD and/or ECDD where relevant, in accordance with paragraphs 2 to 8 of Schedule 3 and chapters 3 to 9 of this Handbook.

(6) Where, following a review, the firm has concluded that the overall risk of a customer has not changed and it considers that the CDD information held appropriately verifies the identity of that customer, in accordance with paragraph 11.9.(3) of this Handbook the firm is not required to re-verify the customer's identity.

(7) When determining whether extra information or documentation is required, particularly in respect of ACDD, the firm should review and research whether existing records contain the required items. The firm may have had a 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.

(8) Where the firm has concluded that the CDD held is not sufficient to provide compliance with Schedule 3 and the Commission Rules, prior to reverting to a customer 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 data, or corroborate any data held.

(9) Where the firm has been unable to obtain any supplementary due diligence information it deems to be required, either from the customer directly or through other means, then it must give consideration to the requirements of paragraph 9 of Schedule 3.

(10) 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 documentation held and the certification provided in connection with that documentation, the firm is not required to re-certify the documentation held, or seek newly certified documentation.

17.7. Collective Investment Schemes – Nominated Firm for Investor CDD

(1) In accordance with paragraph 4.7.1.(1) of this Handbook, each CIS authorised or registered by the Commission must nominate a firm licensed under the POI Law to be responsible for investor CDD.

(2) As required by Rule 4.7.1.(3), the nominated firm must treat the investors in the CIS for which it has been nominated as if they were its customers and conduct customer risk assessments and undertake CDD in accordance with the requirements of paragraphs 3 to 6 of Schedule 3 and chapters 3 to 9 of this Handbook.

(3) Where a fund already holds an authorisation or registration issued by the Commission, the nominated firm must advise the Commission in writing by the 28 February 2018 that it has been so nominated.

Appendix A

Glossary of Terms

The below list of terms includes those defined within paragraph 21 of 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.

"**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.

"**additional customer due diligence**" has the meaning in paragraph 5(3)(b) of Schedule 3.

"**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 an overseas regulatory authority.

"**appropriately qualified**" means that, in respect of a requirement for a person to be appropriately qualified, the person must have appropriate knowledge, skill or experience for the relevant position.

"**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 Supervision (Bailiwick of Guernsey) Law, 1994 and related expressions shall be construed accordingly.

"**Banking Law**" means the Banking Supervision (Bailiwick of Guernsey) Law, 1994 as amended.

"**bearer negotiable instruments**" means monetary instruments in bearer form such as: travellers cheques; negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted.

"**bearer shares**" means negotiable instruments that accord ownership in a corporation to the person who possesses the bearer share certificate.

"**beneficial owner**" has the meaning in paragraphs 21(2) and 21(4) to 21(6) of Schedule 3.

"**Beneficial Ownership Law**" means the Beneficial Ownership of Legal Persons (Guernsey) Law, 2017.

"**Beneficial Ownership Regulations**" means the Beneficial Ownership (Definition) Regulations, 2017.

"**board**" means –

(a) the board of directors of a specified business, where it is a body corporate, or
(b) the senior management of a specified business, where it is not a body corporate.

"**branch offices**" of a specified business are places of business of that specified business which are physically separate from the main place of business of that specified business, and which have no legal personality.

"**British Islands**" means the Bailiwick of Guernsey, 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 an assessment which documents the exposure of a business to ML or FT risks and vulnerabilities, taking into account its –

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

"**the Commission**" means the Guernsey Financial Services Commission established by the Financial Services Commission Law.

"**Code**" means the GFSC 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-

(i) the FATF 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.

"**correspondent banking relationship**" means a business relationship which involves the provision of banking services by one bank ("the correspondent bank") to another bank ("the respondent bank").

"**customer**" means a person or legal arrangement who is seeking –

(a) to establish or has established, a business relationship with a specified business, or
(b) 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) of Schedule 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, including the results of any analysis undertaken.

"**Disclosure Law**" means the Disclosure (Bailiwick of Guernsey) Law, 2007 as amended.

"**document**" includes data or information recorded in any form (including, without limitation, in electronic form).

"**Economic Crime Division**" means the 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 a specified business whether under a contract of employment, a contract for services or otherwise.

"**enactment**" includes a Law, an Ordinance or any subordinate legislation and any provision or portion of a Law, an Ordinance or any subordinate legislation.

"**enhanced customer due diligence**" has the meaning in paragraph 5(3)(a) of Schedule 3.

"**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, e.g. 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 (e.g. a constructive trust).

"**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.

"**Fiduciaries Law**" means the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc. (Bailiwick of Guernsey) Law, 2000 as amended.

"**Financial Crime Compliance Officer**" means a manager, partner or director appointed by a specified business to have responsibility for compliance with policies, procedures and controls to forestall, prevent and detect ML and FT.

"**Financial Crime Reporting Officer**" means a manager, partner or director nominated by a specified business to receive disclosures under Part I of the Disclosure Law and section 15 of the Terrorism Law.

"**financial exclusion**" means individuals are 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 Service**" means the division of the Financial Investigation Unit, comprising those police officers and other persons assigned to the division for the purpose of the receipt, analysis and dissemination within the Bailiwick, and elsewhere, of disclosures which are more commonly known or referred to as suspicious transaction reports or suspicious activity reports.

"**financial services business**" means any business specified in Schedule 1 to the Law and includes, unless the context otherwise requires, a person carrying on such a business.

"**Financial Services Commission Law**" means the Financial Services Commission (Bailiwick of Guernsey) Law, 1987 as amended.

"**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).

"**funds**" means assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable and legal documents or instruments evidencing title to, or interest in, such assets.

"**legal body**" means bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a specified business or otherwise own property.

"**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 or FT and related terms shall be construed accordingly.

"**identification data**" means documents which are from a reliable and independent source.

"**IMII Law**" means the Insurance Managers and Insurance Intermediaries (Bailiwick of Guernsey) Law, 2002 as amended.

"**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 recognized 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**" means a natural person who is, or has been, entrusted with a prominent public function by an international organisation.

"**introducer**" means a specified business, lawyer or accountant who is seeking to establish or has established, on behalf of another person or legal arrangement who is its customer, a business relationship with a specified business.

"**the Law**" means the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended.

"**legal arrangement**" means an express trust or any other vehicle whatsoever which has a similar legal effect.

"**LLP Law**" means the Limited Liability Partnerships (Guernsey) Law, 2013.

"**low risk relationship**" means a business relationship or an occasional transaction which has a low risk of involving ML or FT 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 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.

"**non-Guernsey collective investment scheme**" means any open or closed-ended collective investment scheme established outside the Bailiwick of Guernsey.

"**NRA**" means the National Risk Assessment [published by X on Y] as amended from time to time.

"**NRFSB Law**" means the Non-Regulated Financial Services Businesses (Bailiwick of Guernsey) Law, 2009 as amended.

"**notify**" means notify in writing.

"**occasional transaction**" means any transaction involving more than £10,000, 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.

"**omnibus account**" means a multi-client pooled/omnibus-type account or other arrangement used to collect together funds from a variety of sources for onward investment under the direct control of a financial services business or Appendix C business.

"**payer**" means a natural or legal person 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 or legal person or legal arrangement identified by the payer as the intended recipient of the transfer of funds.

"**payment service provider**" means any business undertaking the activities specified within paragraphs 4 or 5 of Part I of Schedule 1 to the Law.

"**PB Law**" means the Prescribed Business (Bailiwick of Guernsey) Law, 2009 as amended.

"**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.

"**POI Law**" means the Protection of Investors (Bailiwick of Guernsey) Law, 1987 as amended.

"**police officer**" has the meaning in section 51(1) of the Law.

"**politically exposed person**" has the meaning in paragraph 5(3)(c) of Schedule 3.

"**prescribed business**" 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.

"**protector**" has the meaning in section 58 of the Fiduciaries Law.

"**Regulatory Laws**" means –

(a) the Banking Supervision (Bailiwick of Guernsey) Law, 1994 as amended;
(b) the Insurance Business (Bailiwick of Guernsey) Law, 2002 as amended;
(c) the Insurance Managers and Insurance Intermediaries (Bailiwick of Guernsey) Law, 2002 as amended;
(d) the Protection of Investors (Bailiwick of Guernsey) Law, 1987 as amended; and

(e) the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc. (Bailiwick of Guernsey) Law, 2000 as amended.

"**relevant employees**" means any –

(a) member of the board,
(b) member of the management of the specified business, and
(c) employees whose duties relate to the specified business.

"**Relevant Enactments**" means –

(a) the Law,
(b) the Drug Trafficking (Bailiwick of Guernsey) Law, 2000,
(c) the Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011,
(d) the Afghanistan (Restrictive Measures) (Guernsey) Ordinance, 2011
(e) the Afghanistan (Restrictive Measures) (Alderney) Ordinance, 2011
(f) the Afghanistan (Restrictive Measures) (Sark) Ordinance, 2011
(g) the Al-Qaida (Restrictive Measures) (Guernsey) Ordinance, 2013,
(h) the Al-Qaida (Restrictive Measures) (Alderney) Ordinance, 2013,
(i) the Al-Qaida (Restrictive Measures) (Sark) Ordinance, 2013,
(j) the Terrorism Law,
(k) the Disclosure Law,
(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 NRFSB Law,

and such enactments relating to ML and FT 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 and underlying principals of the foundation.

"**risk**" means a risk of ML or FT occurring and "risk assessment" shall be construed accordingly.

"**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 in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.

"**specified business**" has the meaning in paragraph 1(1) of Schedule 3.

"**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.

"**Terrorism Law**" means the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 as amended.

"**Terrorist Asset-Freezing Law**" means the Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011 as amended.

"**terrorist financing**" has the meaning given in the Terrorism Law.

"**transaction document**" has the meaning in paragraph 14 of Schedule 3.

"**transactions**" means, in the general context of the Handbook, an occasional transaction, any customer facing functions, or the handling of business relationships.

"**Transfer of Funds Ordinance**" means the Transfer of Funds (Guernsey, Sark or Alderney) Ordinance, 2017 relevant to the island within which the firm is operating.

"**underlying principal**" has the meaning in paragraphs 21(2) to 21(6) of Schedule 3.

"**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.

"**vested interest**" means an interest which, whether or not currently in possession, is not contingent or conditional on the occurrence of any event.

"**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

Beneficial Ownership of Legal Persons (Guernsey) Law, 2017
[TBC]

Beneficial Ownership (Definition) Regulations, 2017
[TBC]

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
http://www.guernseylegalresources.gg/article/97851/Criminal-Justice-Attempts-Conspiracy-and-Jurisdiction-Bailiwick-of-Guernsey-Law-2006

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
http://www.guernseylegalresources.gg/article/97883/Criminal-Justice-Miscellaneous-Provisions-Bailiwick-of-Guernsey-Law-2006

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

Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) Ordinance, 2017
[TBC]

Disclosure (Bailiwick of Guernsey) Law, 2007
http://www.guernseylegalresources.gg/article/97922/Disclosure-Bailiwick-of-Guernsey-Law-2007-Consolidated-text

Disclosure (Bailiwick of Guernsey) Regulations, 2007
https://www.gfsc.gg/sites/default/files/The-Disclosure-(BoG)-Reg-2007-as-amended.pdf

Drug Trafficking (Bailiwick of Guernsey) Law, 2000
http://www.guernseylegalresources.gg/article/97966/Drug-Trafficking-Bailiwick-of-Guernsey-Law-2000

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
http://www.guernseylegalresources.gg/article/98074/Forgery-and-Counterfeiting-Bailiwick-of-Guernsey-Law-2006

Fraud (Bailiwick of Guernsey) Law 2009
http://www.guernseylegalresources.gg/article/98084/Fraud-Bailiwick-of-Guernsey-Law-2009

Police Property and Forfeiture (Bailiwick of Guernsey) Law, 2006
http://www.guernseylegalresources.gg/article/96675/Police-Property-and-Forfeiture-Bailiwick-of-Guernsey-Law-2006

Prevention of Corruption (Bailiwick of Guernsey) Law, 2003
http://www.guernseylegalresources.gg/article/98459/Prevention-of-Corruption-Bailiwick-of-Guernsey-Law-2003

Terrorism and Crime (Bailiwick of Guernsey) Law, 2002
http://www.guernseylegalresources.gg/article/98996/Terrorism-and-Crime-Bailiwick-of-Guernsey-Law-2002

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

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

Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011
http://www.guernseylegalresources.gg/article/99001/Terrorist-Asset-Freezing-Bailiwick-of-Guernsey-Law-2011-Consolidated-text

Transfer of Funds (Guernsey) Ordinance, 2017 (+Alderney and Sark equivalents)
[TBC]

Website Links

Bailiwick of Guernsey Websites

Guernsey Financial Services Commission
https://www.gfsc.gg/

Financial Investigation Unit (including the Financial Intelligence Service)
http://www.guernseyfiu.gov.gg/

States of Guernsey
https://www.gov.gg/

We Are Guernsey (previously Guernsey Finance)
https://www.weareguernsey.com/

Other Official Websites

Asia/Pacific Group on Money Laundering
http://www.apgml.org/

Basel Committee for Banking Supervision
http://www.bis.org/bcbs/index.htm

British Bankers Association
https://www.bba.org.uk/

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

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
http://www.gifcs.org/

Group of States against Corruption (Council of Europe)
http://www.coe.int/t/dghl/monitoring/greco/default_en.asp

HM Treasury
https://www.gov.uk/government/organisations/hm-treasury

HM Treasury – Office of Financial Sanctions Implementation
https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation

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 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/

United Kingdom Financial Conduct Authority
https://www.fca.org.uk/

United Kingdom Foreign and Commonwealth Office
https://www.gov.uk/government/organisations/foreign-commonwealth-office

United Kingdom Joint Money Laundering Steering Group
http://www.jmlsg.org.uk/

United Kingdom National Crime Agency
http://www.nationalcrimeagency.gov.uk/

United Kingdom Office of Public Sector Information
http://www.opsi.gov.uk/psi/

United Nations
http://www.un.org/en/index.html

United Nations Office on Drugs and Crime
http://www.unodc.org/

World Bank
http://www.worldbank.org/

World Customs Organization
http://www.wcoomd.org/en.aspx

Appendix C

Equivalent Jurisdictions

Australia	http://www.fatf-gafi.org/countries/#Australia
Austria	http://www.fatf-gafi.org/countries/#Austria
Belgium	http://www.fatf-gafi.org/countries/#Belgium
Bermuda	https://www.cfatf-gafic.org/index.php/member-countries/a-d/Bermuda
Bulgaria	http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Bulgaria_en.asp
Canada	http://www.fatf-gafi.org/countries/#Canada
Cayman Islands	http://www.fatf-gafi.org/countries/#CaymanIslands
Cyprus	http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Cyprus_en.asp
Denmark	http://www.fatf-gafi.org/countries/#Denmark
Estonia	http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Estonia_en.asp
Finland	http://www.fatf-gafi.org/countries/#Finland
France	http://www.fatf-gafi.org/countries/#France
Germany	http://www.fatf-gafi.org/countries/#Germany
Gibraltar	http://www.imf.org/external/pubs/cat/longres.aspx?sk=20952
Greece	http://www.fatf-gafi.org/countries/#Greece
Hong Kong	http://www.fatf-gafi.org/countries/#HongKong(China)
Hungary	http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Hungary_en.asp
Iceland	http://www.fatf-gafi.org/countries/#Iceland
Ireland	http://www.fatf-gafi.org/countries/#Ireland
Isle of Man	http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Isle_of_Man_en.asp
Italy	http://www.fatf-gafi.org/countries/#Italy
Japan	http://www.fatf-gafi.org/countries/#Japan
Jersey	http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Jersey_en.asp
Latvia	http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Latvia_en.asp
Liechtenstein	http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Liechtenstein_en.asp
Lithuania	http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Lithuania_en.asp
Luxembourg	http://www.fatf-gafi.org/countries/#Luxembourg
Malta	http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Malta_en.asp
Netherlands	http://www.fatf-gafi.org/countries/#NetherlandsKingdomof
New Zealand	http://www.fatf-gafi.org/countries/#NewZealand
Norway	http://www.fatf-gafi.org/countries/#Norway
Portugal	http://www.fatf-gafi.org/countries/#Portugal
Singapore	http://www.fatf-gafi.org/countries/#Singapore
Slovenia	http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Slovenia_en.asp
South Africa	http://www.fatf-gafi.org/countries/#SouthAfrica
Spain	http://www.fatf-gafi.org/countries/#Spain
Sweden	http://www.fatf-gafi.org/countries/#Sweden
Switzerland	http://www.fatf-gafi.org/countries/#Switzerland
United Kingdom	http://www.fatf-gafi.org/countries/#UnitedKingdom
United States of America	http://www.fatf-gafi.org/countries/#UnitedStates

Appendix C to this Handbook was established to reflect those countries or territories which the Commission considers require regulated FSBs to have in place standards to combat ML and FT consistent with the FATF Recommendations and where such FSBs are supervised for compliance with those requirements. It was also designed as a mechanism to recognise the geographic spread of the customers of the Bailiwick's finance sector and is reviewed periodically with countries or territories being added as appropriate.

The fact that a country or territory has requirements to combat ML and FT that are consistent with the FATF Recommendations means only that the necessary legislation and other means of ensuring compliance with the FATF Recommendations is in force in that country or territory. It does not provide assurance that a particular overseas FSB 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 should use its commercial judgement in considering whether or not to deal with a regulated FSB and may, if it wishes, impose higher standards than the minimum standards identified in this Handbook.

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 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 ML and FT 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 chapter 10 of this Handbook. In this respect the firm can still accept introduced business relationships, provided the requirements in section 10.6. of this Handbook are met.

Introduced Business - Group Introducers

Further information in respect of Appendix C and the treatment of an Appendix C business can be found in section 9.5. of this Handbook:

Simplified Customer Due Diligence – Appendix C Business