Guernsey Financial
Services Commission

HANDBOOK FOR FINANCIAL SERVICES BUSINESSES ON COUNTERING FINANCIAL CRIME AND TERRORIST FINANCING

15 December 2007
(updated June 2017)

CONTENTS

PART 1 Page

PART 1 – REGULATORY REQUIREMENTS AND GUIDANCE NOTES

CHAPTER 1 – INTRODUCTION

Sections in this Chapter

1 INTRODUCTION

1. The laundering of criminal proceeds and the financing of terrorism through the financial 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 financial services businesses in order to benefit from such proceeds or financing. 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 of Guernsey (Guernsey) as a well-respected international financial centre depends on its ability to prevent the abuse of its financial services sector. Descriptions of money laundering and terrorist financing are provided in Appendix H to this Handbook.

1.1 Background and Scope

2. The Guernsey authorities are committed to ensuring that money launderers, terrorists, those financing terrorism and other criminals, cannot launder the proceeds of crime through Guernsey, or otherwise use Guernsey's finance sector. The Guernsey Financial Services Commission (the Commission) endorses the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation issued by the Financial Action Task Force (FATF). The Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing (the Handbook) is a statement of the standards expected by the Commission of all financial services businesses in Guernsey to ensure Guernsey's compliance with the FATF's standards.

3. Under section 1(1) of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 all offences that are indictable under the law of the Bailiwick are considered to be predicate offences and therefore funds obtained by committing a predicate offence are considered to be the proceeds of crime. Under Bailiwick law all offences are indictable except for some minor offences, which mainly concern public order and road traffic. Therefore, the range of predicate offences is extremely wide and includes but is not limited to the following:

- participation in an organised criminal group and racketeering;
- terrorism, including terrorist financing;
- trafficking in human beings and migrant smuggling;
- sexual exploitation, including sexual exploitation of children;
- illicit trafficking in narcotic drugs and psychotropic substances;
- illicit arms trafficking;
- illicit trafficking in stolen and other goods;
- corruption and bribery;
- fraud and tax evasion;
- counterfeiting and piracy of products;
- environmental crime;
- murder, grievous bodily injury;
- kidnapping, illegal restraint and hostage taking;

- robbery or theft;
- smuggling;
- extortion;
- forgery;
- piracy; and
- insider trading and market manipulation

4. Guernsey's anti-money laundering and countering the financing of terrorism (AML/CFT) legislation (and by extension, the Handbook) applies to all financial services businesses conducting financial services business in Guernsey. This includes Guernsey-based branches and offices of companies incorporated outside Guernsey conducting financial services business in Guernsey.

1.2 Purpose of the Handbook

5. The Handbook has been issued by the Commission and, together with Statements issued by the Commission, contains the rules and guidance referred to in Regulation 3(2) of the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2007 as amended (the Regulations), section 15(8) of the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 as amended, section 15 of the Disclosure (Bailiwick of Guernsey) Law, 2007 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.

6. The Handbook is issued to assist financial services businesses to comply with the requirements of the relevant legislation concerning money laundering, terrorist financing and related offences to prevent the Bailiwick's financial system from being used in the laundering of money or the financing of terrorism. The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended and the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 as amended states that the Guernsey courts shall take account of rules made and guidance given by the Commission in determining whether or not a person has complied with the Regulations.

7. The Guernsey AML/CFT framework includes the following legislation, which is referred to in the Handbook as the relevant enactments:

- The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended;
- The Drug Trafficking (Bailiwick of Guernsey) Law, 2000 as amended;
- The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 as amended;
- The Transfer of Funds (Guernsey) Ordinance, 2017;
- The Transfer of Funds (Alderney) Ordinance, 2017;
- The Transfer of Funds (Sark) Ordinance, 2017;
- The Disclosure (Bailiwick of Guernsey) Law, 2007 as amended;

- The Disclosure (Bailiwick of Guernsey) Regulations, 2007 as amended;
- The Terrorism and Crime (Bailiwick of Guernsey) Regulations, 2007 as amended;
- The Registration of Non-Regulated Financial Services Businesses (Bailiwick of Guernsey) Law, 2008 as amended;
- The Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011
- The Al-Qaida and Taliban (Freezing of Funds) (Guernsey) Ordinance, 2011

and such enactments relating to money laundering or terrorist financing as may be enacted from time to time in the Bailiwick.

8. The Regulations include requirements relating to:

- risk assessment and mitigation;
- undertaking customer due diligence (CDD);
- monitoring customer activity and ongoing CDD;
- reporting suspected money laundering and terrorist financing activity;
- staff screening and training;
- record keeping; and
- ensuring compliance, corporate responsibility and related requirements.

9. For any financial services business, whether regulated by the Commission or registered with the Commission, the primary consequences of any significant failure to meet the standards required by the Regulations, the Handbook and the relevant enactments will be legal ones.

10. As regards a financial services business regulated by the Commission, the Commission is entitled to take such failure into consideration in the exercise of its judgment as to whether the financial services business and its directors and managers have satisfied the minimum criteria for licensing. In particular, in determining whether a firm is carrying on its business with integrity and skill and whether a person is fit and proper, the Commission must have regard to compliance with the Regulations, related rules in the Handbook and the relevant enactments.

11. As regards a financial services business which is not regulated by, but is registered with, the Commission, the Commission is entitled to consider compliance with the Regulations, the Handbook and the relevant enactments when exercising its judgement in considering the continuing registration of a financial services business.

1.3 Contents of the Handbook

12. The Handbook is divided into three parts. The text in Part 1 applies to all Guernsey financial services businesses. Part 2 provides material for a number of

specific industry sectors, which supplements the generic text contained in Part 1. Part 3 contains appendices and a glossary of terms.

13. The full text of the Regulations is set out in Appendix F. That text is definitive. Any paraphrasing of that text within Part 1 or 2 of the Handbook represents the Commission's own explanation of the Regulations and is for the purposes of information and assistance only. That paraphrasing does not detract from the legal effect of the Regulations or from their enforceability by the courts. In case of doubt you are advised to consult a Guernsey Advocate.

14. Part 1 of the Handbook takes a two-level approach:

- Level one (**Commission Rules**) sets out how the Commission requires financial services businesses to meet the Regulations. Compliance with the Commission Rules must be taken into account by the courts when considering compliance with the Regulations (which are legally enforceable and a contravention of which can result in prosecution). In addition, the Commission can take enforcement action under the regulatory laws for any contravention of the Commission Rules in respect of those financial services businesses licensed or authorised under those laws. The Commission can also take enforcement action under the Registration of Non-Regulated Financial Services Businesses (Bailiwick of Guernsey) Law, 2008 as amended in respect of those financial services businesses registered with the Commission under that law. In addition, the Commission can take enforcement action under the regulatory laws for any contravention of the Commission Rules in respect of those financial services businesses licensed or authorised under those laws and under the Financial Services Commission Law.
- Level two (**Guidance**) presents ways of complying with the Regulations and the Commission Rules. A financial services business 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 financial services business, so long as it can demonstrate that such measures also achieve compliance with the Regulations and the Commission Rules.

15. When obligations in the Regulations are explained or paraphrased in the Handbook, and where the Commission's Rules are set out in the Handbook, the term **must** is used, indicating that these provisions are **mandatory** and subject to the possibility of prosecution (in the case of a contravention of the Regulations) as well as regulatory sanction and any other applicable sanctions.

16. Information on the Regulations and, where appropriate, the text of the most relevant Regulations are shown in a box on a white background at the front of each chapter.

17. The text of the Commission Rules is presented in shaded boxes throughout each chapter of the Handbook for ease of reference.

18. In other cases, i.e. Guidance, the Handbook uses the terms **should** or **may** to indicate ways in which the requirements of the Regulations and the Commission Rules may be satisfied, but allowing for alternative means of meeting the

requirements. References to "must", "should" and "may" in the text must therefore be construed accordingly.

19. The Commission will from time to time update the Handbook to reflect new legislation, developments in the finance sector, changes to international standards and good practice and the Regulations.

20. The Handbook is not intended to provide an exhaustive list of appropriate and effective policies, procedures and controls to counter money laundering and the financing of terrorism. The structure of the Handbook is such that it permits a financial services business to adopt a risk-based approach appropriate to its particular circumstances. The financial services business should give consideration to additional measures that may be necessary to prevent its exploitation and that of its services/products and delivery channels by persons seeking to carry out money laundering or terrorist financing.

1.4 Risk-Based Approach

21. A risk-based approach is a systematic approach to risk management and involves:

- risk identification and assessment – taking account of the customer and the business relationship or occasional transaction and of the product/service/delivery channel to identify the money laundering and terrorist financing risk to the financial services business;
- risk mitigation – applying appropriate and effective policies, procedures and controls to manage and mitigate the risks identified;
- risk monitoring – monitoring the effective operation of a financial services business' policies, procedures and controls; and
- policies, procedures and controls – having documented policies, procedures and controls to ensure accountability to the board and senior management.

22. As part of the risk-based approach, financial services businesses are actively encouraged by the Commission to develop modern and secure techniques of money management as a means of encouraging the replacement of cash transfers. In addition, the Commission discourages the inappropriate use of cash collections and supports the maintenance of registers by financial services businesses which record the value and reasons for cash collections.

23. It is important to realise that various sectors in the financial services industry – whether in terms of products/services or delivery channel or typical customers, can differ materially. An approach to preventing money laundering and terrorist financing that is appropriate in one sector may be inappropriate in another.

24. A financial services business should be able to take such an approach to the risk of being used for the purposes of money laundering and terrorist financing and to ensure that its policies, procedures and controls are appropriately designed and implemented and are effectively operated to reduce the risk of the financial services business being used in connection with money laundering or terrorist financing.

CHAPTER 2 – CORPORATE GOVERNANCE

Key Regulations

Sections in this Chapter

REGULATIONS

The requirements of the Regulations to which the rules and guidance in this chapter particularly relate are:

- Regulation 12, which provides for the appointment of a money laundering reporting officer and the reporting of suspicion. See chapter 10.
- Regulation 15, which makes provisions in relation to the review of compliance. See below.

Regulation 15

15. (1) A financial services business must, in addition to complying with the preceding requirements of these Regulations –

(a) establish such other policies, procedures and controls as may be appropriate and effective for the purposes of forestalling, preventing and detecting money laundering and terrorist financing,

(b) establish and maintain an effective policy, for which responsibility must be taken by the board, for the review of its compliance with the requirements of these Regulations and such policy shall include provision as to the extent and frequency of such reviews,

(c) ensure that a review of its compliance with these Regulations is discussed and minuted at a meeting of the board at appropriate intervals, and in considering what is appropriate a financial services business must have regard to the risk taking into account –

(i) the size, nature and complexity of the financial services business,
(ii) its customers, products and services, and
(iii) the ways in which it provides those products and services,

(d) subject to paragraph (2), ensure that any of its branch offices and, where it is a body corporate, any body corporate of which it is the majority shareholder, which, in either case, is a financial services business in any country or territory outside the Bailiwick, complies there with –

(i) the requirements of these Regulations, and

(ii) any requirements under the law applicable in that country or territory which are consistent with the Financial Action Task Force Recommendations on Money Laundering,

provided that, where requirements under subparagraphs (i) and (ii) differ, a financial services business must ensure that the requirement which provides the highest standard of compliance by reference to the Financial Action Task Force Recommendations on Money Laundering, is complied with.

(2) The obligation under paragraph (1) (d) applies to the extent that the law of the relevant country or territory allows and if the law of that country or territory does not so allow in relation to any requirement of these Regulations, the financial services business must notify the Commission accordingly.

2. CORPORATE GOVERNANCE

A financial services business must comply with the Rules in addition to the Regulations. The Rules are boxed and shaded for ease of reference. A financial services business should note that the Court must take account of the Rules and Guidance issued by the Commission in considering compliance with the Regulations.

2.1 Objectives

25. Corporate governance refers to the manner in which boards of directors and senior management oversee the financial services business. This chapter, together with the Regulations, provides the framework for oversight of the policies, procedures and controls of a financial services business to counter money laundering and terrorist financing.

2.2 Corporate Governance

26. References in this chapter to "the Board" must be read as meaning the senior management of the financial services business where the business is not a company, but is, for example, a firm or partnership.

2.3 Board Responsibility for Oversight of Compliance

27. The Board of the financial services business has effective responsibility for compliance with the Regulations and the Handbook and references to compliance in this Handbook generally, are to be taken as references to compliance with the Regulations and the Handbook. In particular the Board must take responsibility for the policy on reviewing compliance and must consider the appropriateness and effectiveness of compliance and the review of compliance at appropriate intervals.
28. A financial services business must also ensure that there are appropriate and effective policies, procedures and controls in place which provide for the Board to meet its obligations relating to compliance review, in particular the Board must:
    - ensure that the compliance review policy takes into account the size, nature and complexity of the business and includes a requirement for sample testing of the effectiveness and adequacy of the policies, procedures and controls including where aspects of the due diligence process are undertaken via electronic methods and systems;
    - consider whether it would be appropriate to maintain a separate audit function to assess the adequacy and effectiveness of the area of compliance;
    - ensure that when a review of compliance is discussed by the Board at appropriate intervals the necessary action is taken to remedy any identified deficiencies;
    - ensure that the financial services business is meeting its obligation that its branches and subsidiaries operating outside the Bailiwick comply with the Regulations and applicable local law which is consistent with the FATF Recommendations;
    - provide adequate resources either from within the financial services business, within the group, or externally to ensure that the AML/CFT policies,

procedures and controls of the financial services business are subject to regular monitoring and testing as required by the Regulations;
- provide adequate resources to enable the MLRO to perform his duties; and
- take appropriate measures to keep abreast of and guard against the use of technological developments and new methodologies in money laundering and terrorist financing schemes.

29. The Board may delegate some or all of its duties but must retain responsibility for the review of overall compliance with AML/CFT requirements as required by Regulation 15.

2.3.1 Liaison with the Commission

30. The Board of a financial services business must ensure that the Commission is advised of any material failure to comply with the provisions of the Regulations and the rules in the Handbook and of any serious breaches of the policies, procedures or controls of the financial services business.

2.3.2 Financial services business conducted outside Guernsey

31. Where a branch or subsidiary is unable to observe the appropriate AML/CFT measures because local laws, Regulations or other measures prohibit this, the Regulations require that a financial services business informs the Commission.

32. A financial services business must be aware that this inability to observe the appropriate AML/CFT measures is particularly likely to occur in countries or territories which do not or insufficiently apply the FATF Recommendations.

2.3.3 Outsourcing

33. It should be noted that whether a financial services business carries out a function itself, or outsources the function to a third party (either in Guernsey or overseas, or within its group or externally) the financial services business remains responsible for compliance with the Regulations in Guernsey and the requirements of the Handbook. A financial services business cannot contract out of its statutory and regulatory responsibilities to prevent and detect money laundering and terrorist financing.

34. Where a financial services business wishes to outsource functions, it should make an assessment of any potential money laundering and financing of terrorism risk, maintain a record of the assessment, monitor the perceived risk, and ensure that relevant policies, procedures and controls are and continue to be in place at the outsourced business.

35. Where a financial services business is considering the outsourcing of compliance functions and/or providing the MLRO with additional support from third parties, from elsewhere within the group or externally, then the business should:

- consider and adhere to the Commission's policy on outsourcing;

- ensure that roles, responsibilities and respective duties are clearly defined and documented;
- ensure that the MLRO, any deputy MLRO, other third parties and all employees understand the roles, responsibilities and respective duties of all parties.

2.4 The Money Laundering Reporting Officer

36. In larger financial services businesses, because of their size, nature and complexity, the appointment of one or more appropriately qualified persons as permanent deputy MLROs may be necessary.

37. The MLRO and any deputy MLROs that are appointed must:

- be a natural person;
- be employed by the financial services business. In the case of managed or administered businesses it is acceptable for an employee of the manager or administrator of the business to be appointed as the MLRO/deputy MLRO;
- be resident in Guernsey;
- be the main point of contact with the Financial Intelligence Service (FIS) in the handling of disclosures;
- have sufficient resources to perform his duties;
- have access to the CDD records;
- be available on a day to day basis (see section 2.4.1);
- receive full cooperation from all staff;
- report directly to the Board;
- have regular contact with the Board to ensure that the Board is able to satisfy itself that all statutory obligations and provisions in the Handbook are being met and that the financial services business is taking sufficiently robust measures to protect itself against the potential risk of being used for money laundering and terrorist financing; and
- be fully aware of both his obligations and those of the financial services business under the Regulations, the relevant enactments and the Handbook.

2.4.1 Nominated officer

38. In order to meet the requirements of Regulation 12(b), a financial services business must nominate another person to receive disclosures in the absence of the MLRO and must communicate the name of the nominated officer to the employees. The nominated person must be of at least management level and must be appropriately qualified.

CHAPTER 3 – A RISK-BASED APPROACH

Key Regulations

Sections in this Chapter

REGULATIONS

The requirements of the Regulations to which the rules and guidance in this chapter particularly relate are:

- Regulation 3, which provides for a financial services business to identify and assess the risks of money laundering and terrorist financing and to ensure that its policies, procedures and controls are effective and appropriate to the assessed risk. See below.
- Regulation 15, which makes provisions in relation to the review of compliance. See chapter 2.

Regulation 3

3. (1) A financial services business must-

(a) carry out and document a suitable and sufficient money laundering and terrorist financing business risk assessment which is specific to the financial services business-

(i) as soon as reasonably practicable after these Regulations come into force, or

(ii) in the case of a financial services business which only becomes such on or after the date these Regulations come into force, as soon as reasonably practicable after it becomes such a business, and

(b) regularly review its business risk assessment, at a minimum annually, so as to keep it up to date and, where, as a result of that review, changes to the business risk assessment are required, it must make those changes,

(2) A financial services business must-

(a) prior to the establishment of a business relationship or the carrying out of an occasional transaction, undertake a risk assessment of that proposed business relationship or occasional transaction,

(b) regularly review any risk assessment carried out under subparagraph (a) so as to keep it up to date and, where changes to that risk assessment are required, it must make those changes, and

(c) ensure that its policies, procedures and controls on forestalling, preventing and detecting money laundering and terrorist financing are appropriate and effective, having regard to the assessed risk.

(3) A financial services business must have regard to

(a) any relevant rules and guidance in the Handbook and,

(b) any notice or instruction issued by the Commission under the Law,

in determining, for the purposes of these Regulations, what constitutes a high or low risk.

3 A RISK-BASED APPROACH

A financial services business must comply with the Rules in addition to the Regulations. The Rules are boxed and shaded for ease of reference. A financial services business should note that the Court must take account of the Rules and Guidance issued by the Commission in considering compliance with the Regulations.

3.1 Objectives

39. Reference in this chapter to "the Board" must be read as meaning the senior management of the financial services business where the business is not a company, but is, for example, a firm or partnership.

40. The Board and senior management of any business are responsible for managing the business effectively. They are in the best position to evaluate all potential risks. The Board and senior management of a financial services business are accustomed to applying proportionate risk-based policies across different aspects of their business.

41. It should be noted that in respect of administered entities, the responsibility is retained by the Board and senior management of the administered entity and not transferred to the administrator of these entities.

42. This chapter, together with the Regulations, is designed to assist a financial services business to take such an approach to the risk of its products and services being used for the purposes of money laundering and terrorist financing and to ensure that its policies, procedures and controls are appropriately designed and implemented and are effectively operated to reduce the risk of the financial services business being used in connection with money laundering and terrorist financing.

43. In order to meet the requirements of Regulation 3 a financial services business must have regard to any relevant rules and guidance in assessing the risk of a business relationship or occasional transaction particularly in respect of higher risk relationships or transactions.

3.2 Benefits of a Risk-Based Approach

44. No system of checks will detect and prevent all money laundering or terrorist financing. A risk-based approach will, however, serve to balance the cost burden placed on individual businesses and on their customers with a realistic assessment of the threat of the business being used in connection with money laundering or terrorist financing. It focuses the effort where it is needed and has most impact.

45. To assist the overall objective to prevent the abuse of the financial services sector, a risk-based approach:

- recognises that the money laundering/terrorist financing threat to a financial services business varies across its customers, countries/territories, products/services and delivery channels;
- allows the Board and senior management to differentiate between their customers in a way that matches the risk in their particular business;
- allows the Board and senior management to apply their own approach to the policies, procedures and controls of the financial services business in particular circumstances;
- helps to produce a more cost-effective system;
- promotes the prioritisation of effort and activity by reference to the likelihood of money laundering or terrorist financing taking place;
- reflects experience and proportionality through the tailoring of effort and activity to risk; and
- allows a financial services business to apply the Handbook sensibly and to consider all relevant factors.

46. A risk-based approach takes a number of discrete steps in assessing the most cost-effective and proportionate way to manage the money laundering and terrorist financing risks facing a financial services business by:

- identifying and assessing the money laundering and terrorist financing risks presented by the particular customers, products/services, delivery channels and geographical areas of operation of the financial services business;
- managing and mitigating the assessed risks by the application of appropriate and effective policies, procedures and controls;
- monitoring and improving the effective operation of the policies, procedures and controls; and
- documenting, as appropriate, the policies, procedures and controls to ensure accountability to the Board and senior management.

3.3 Identifying and Assessing the Risks

47. A risk-based approach starts with the identification and assessment of the risk that has to be managed. In the context of the Handbook a risk-based approach requires a financial services business to assess the risks of how it might be involved in money laundering or terrorist financing taking into account its customers, products and services and the ways in which it provides those services.

48. A financial services business should ask itself what is the threat of it being used for money laundering or terrorist financing. For example:

- What risk is posed/mitigated by the customers of the financial services business, taking into account:
    - their wealth;
    - their influence;
    - their geographical origin;
    - the complexity of their transaction structures;

- the complexity of legal persons and legal arrangements;
- whether they were introduced to the financial services business; and
- any unwillingness of customers who are not individuals to give the names of their underlying owners and principals.

- What risk is posed/mitigated by the products/services offered by the financial services business? For example:

  - whether the value of a transaction is particularly high;
  - whether payments to third parties are allowed;
  - whether the product/service/structure is of particular, or unusual, complexity.

3.4 Business Risk Assessment – Management and Mitigation

49. In order to ensure its policies, procedures and controls on anti-money laundering and terrorist financing are appropriate and effective, having regard to the assessed risk, a financial services business must ask itself what measures it can adopt, and to what extent, to manage and mitigate the identified risks cost-effectively.

50. These measures may, for example, include:

- varying the CDD procedures in respect of customers appropriate to their assessed money laundering and terrorist financing risk;
- requiring the quality of evidence – documentary/electronic/third party assurance – to be of a certain standard;
- obtaining additional customer or business relationship information where this is appropriate to their assessed money laundering or terrorist financing risk, for example, identifying and understanding where a customer's funds and wealth come from;
- monitoring ongoing CDD, existing customer accounts and ongoing business relationships.

51. The responses to the questions set out in section 3.3, or to similar questions, will be a useful framework for the process whereby a financial services business, having assessed the risk to its business, is able to tailor its policies, procedures and controls on the countering of money laundering and terrorist financing.

3.5 Relationship Risk Assessment – Management and Mitigation

52. The policies, procedures and controls of each financial services business towards the identification and assessment of risk in its customer base must be appropriate, effective, documented and approved at Board level.

53. For a financial services business to consider the extent of its potential exposure to the risk of money laundering and terrorist financing it must assess the risk of any proposed business relationship or occasional transaction. Based on this

assessment, the financial services business must decide whether or not to accept each business relationship and whether or not to accept any instructions to carry out any occasional transactions.

54. In addition, the assessment will allow a financial services business to determine, on a risk basis, the extent of identification information (and other CDD information) that must be obtained, how that information will be verified, and the extent to which the resulting business relationship will be monitored.

55. When assessing the risk of a proposed business relationship or occasional transaction a financial services business must ensure that all the relevant risk factors are considered before making a determination on the level of overall assessed risk.

56. Information which must be taken into consideration when undertaking a relationship risk assessment includes but is not limited to:

- the identity of the customer, beneficial owners and underlying principals;
- the associated geographic areas;
- the products/services being provided and the delivery channel;
- 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 business relationship or occasional transaction;
- the type, volume, value and regularity of transactions and activity expected; and
- the expected duration of the business relationship[i].

57. Where one or more aspects of the business relationship or occasional transaction indicates a high risk of money laundering or terrorist financing but the financial services business does not assess the overall risk as high because of strong and compelling mitigating factors, the financial services business must identify the mitigating factors and, along with the reasons for the decision, document them.

58. A financial services business must ensure that any proposed or existing business relationship or any proposed occasional transaction which:

- has characteristics identified in Regulation 5(1)(a) to (c); or
- is connected to any of the countries or territories listed in Part A or Part C of Instructions on Business from Sensitive Sources issued by the Commission;

is designated as high risk.

59. A financial services business must have documented procedures which will 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 its operation.

60. Such procedures may provide for standardised profiles to be used where the financial services business has satisfied itself, on reasonable grounds, that such an

i. See FAQ published on 30 June 2017: https://www.gfsc.gg/commission/financial-crime/faqs

approach effectively assesses the risk for each particular business relationship or occasional transaction. However, a financial services business with a diverse customer base or where a wide range of products and services are available 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.

61. Whatever method is used to assess the risk of a business relationship or occasional transaction there must be clear documented evidence as to the basis on which the assessment has been made.

3.5.1 Business from Sensitive Sources Notices, Instructions, etc.

62. From time to time the Commission issues Business from Sensitive Sources Notices, Advisory Notices, Instructions and Warnings which highlight potential risks arising from particular sources of business. A financial services business must ensure that it visits the Commission's website and apprise itself of the available information on a regular basis. Additionally, this information, which is updated as necessary, together with sanctions legislation applicable in the Bailiwick, must be taken into consideration when seeking to create a relationship risk profile.

63. Further information on two of the relevant enactments, for the purposes of this Handbook the Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011 ("Terrorist Law 2011") and the Al-Qaida and Taliban (Freezing of Funds) (Guernsey) Ordinance, 2011 ("Al-Qaida Ordinance 2011") can be found in chapters 14 and 16.

64. Care must be taken when dealing with customers, beneficial owners and underlying principals from countries or territories which are associated with the production, processing and trafficking of illegal drugs. Financial services businesses must also exercise a higher degree of awareness of the potential problems associated with taking on politically sensitive and other customers from countries or territories where bribery and corruption are widely considered to be prevalent.

65. Countries or territories that do not or insufficiently apply the FATF Recommendations and other high risk countries or territories are dealt with in section 5.5 of the Handbook.

3.5.2 Inherent risks

66. A financial services business must have regard to the attractiveness to money launderers of the availability of complex products and services that operate within reputable and secure wealth management environments that are familiar with high value transactions. The following factors contribute to the increased vulnerability of wealth management:

- wealthy customers, private banking customers and powerful customers – such customers may be reluctant or unwilling to provide adequate documents,

details and explanations;

- multiple accounts and complex accounts – customers often have many accounts in more than one jurisdiction, either within the same firm or group, or with different firms;
- movement of funds – the transmission of funds and other assets by private customers often involve high value transactions, requiring rapid transfers to be made across accounts in different countries and regions of the world.

67. In order to counter the perceived and actual risks of such relationships, a financial services business must ensure it recognises, manages and mitigates the potential risks arising from relationships with high net worth customers.

3.5.3 Profile indicators

68. Regulations 5 and 6 and the rules in chapters 5 and 6 of the Handbook set out the particular circumstances in relation to the assessment of a proposed business relationship or occasional transaction as having either a high or low risk of money laundering and terrorist financing.

69. This paragraph provides examples of low risk indicators for customers and for products and services which a financial services business may consider when preparing a profile.

(a) Customers – Low Risk Indicators

- customers whose funds are part of a pooled client money account held in the name of an Appendix C business (see the definition in Appendix C to the Handbook);
- customers who are actively employed with a regular source of income which is consistent with the employment being undertaken;
- customers who are locally resident retail customers who have a business relationship which is understood by the financial services business; and
- customers represented by those whose appointment is subject to court approval or ratification (such as executors).

(b) Products and services – Low Risk Indicators

- products where the provider does not permit third party investment or repayment and the ability to make or receive payments to or from third parties is restricted;
- life insurance policies where the annual premium is no more than £1,000 or a single premium of no more than £2,500;
- insurance policies for pension schemes if there is no surrender clause and the policy cannot be used for collateral; and
- regular payment savings or investment/insurance products.

70. This paragraph provides examples of high risk indicators for customers and for products and services which a financial services business may consider when preparing a profile.

(a) Customers – High Risk Indicators

- complex ownership structures, which can make it easier to conceal underlying beneficial owners and beneficiaries;
- structures where there is no apparent legitimate economic or other rationale;
    - customers or structures which are associated with a specific industry activity which carries a higher exposure to the possibility of bribery and corruption (such as in natural resource extraction, infrastructure construction or the defence industry);an individual who may be regarded as a commercially exposed person because of his or her position as a senior executive of a well known commercial enterprise;
    - customers based in, or conducting business in or through, a country or territory with known higher levels of bribery and corruption, or organised crime, or involved in illegal drug production/processing/distribution, or associated with terrorism; involvement of an introducer from a country or territory which does not have an adequate AML/CFT infrastructure;
    - where a customer wants a product or service 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 buying the product or service abroad;
    - requests to adopt undue levels of secrecy with a transaction; and
    - business relationships or occasional transactions where the source of wealth and source of funds cannot be easily verified or where the audit trail has been deliberately broken and/or unnecessarily layered.

(b) Products and Services – High Risk Indicators

- complex structures of legal persons and/or legal arrangements;
- hold mail or retained mail arrangements;
- safe custody arrangements;
- significant and/or frequent cash transactions;
- high value balances or investments, which are disproportionately large to that particular customer, product or service set;
- bearer shares and other bearer instruments; and
- inappropriate delegation of authority.

3.6 Monitoring the Effectiveness of Policies, Procedures and Controls

71. The financial services business' compliance review policy must make provision for a review of the following elements to ensure their appropriateness and effectiveness:

    - the procedures surrounding the products/services offered by the financial services business;
    - the CDD requirements in place including where provided through the use of any electronic method or system for establishing a new business relationship or undertaking an occasional transaction;
    - staff screening and training; and

- monitoring compliance arrangements.

3.7 Documentation

72. Documentation of the results achieved by taking the steps set out in sections 3.3 to 3.6 will assist the financial services business to demonstrate:

- how it identifies and assesses the risks of being used for money laundering or terrorist financing;
- how it agrees and implements appropriate and effective policies, procedures and controls to manage and mitigate the risk;
- how it monitors and improves the effectiveness of its policies, procedures and controls; and
- how it ensures accountability of the Board and senior management on the operation of its policies, procedures and controls process.

CHAPTER 4 – CUSTOMER DUE DILIGENCE

Key Regulations

Sections in this Chapter

REGULATIONS

The requirements of the Regulations to which the rules and guidance in this chapter particularly relate are:

- Regulation 3, which provides for a financial services business to identify and assess the risks of money laundering and terrorist financing and to ensure that its policies, procedures and controls are effective and appropriate to the assessed risk. See chapter 3.
- Regulation 4, which provides for the required customer due diligence measures, when they should be applied and to whom they should be applied. See below.
- Regulation 7, which provides for the timing of identification and verification of identity. See below.
- Regulation 8, which makes provisions in relation to anonymous accounts and shell banks. See chapter 8.
- Regulation 9, which provides for the non-compliance with customer due diligence measures. See below.
- Regulation 10, which provides for the customer due diligence measures to be undertaken in introduced business relationships. See below.
- Regulation 15, which makes provisions in relation to the review of compliance. See chapter 2.

Regulation 4

4.(1) A financial services business shall, subject to the following provisions of these Regulations, ensure that the steps in paragraph (3) are carried out -

(a) when carrying out the activities in paragraphs (2)(a) and (b) and in the circumstances in paragraphs (2)(c) and (d), and

(b) in relation to a business relationship established prior to the coming into force of these Regulations -

(i) in respect of which there is maintained an anonymous account or an account in a fictitious name, as soon as possible after the coming into force of these Regulations and in any event before such account is used again in any way, and

(ii) where it does not fall within subparagraph (i) and to the extent that such steps have not already been carried out, at appropriate times on a risk-sensitive basis.

(2) The activities and circumstances referred to in paragraph (1) are -

(a) establishing a business relationship,

(b) carrying out an occasional transaction,

(c) where the financial services business knows or suspects or has reasonable

grounds for knowing or suspecting -

(i) that, notwithstanding any exemptions or thresholds pursuant to these Regulations, any party to a business relationship is engaged in money laundering or terrorist financing, or

(ii) that it is carrying out a transaction on behalf of a person, including a beneficial owner or underlying principal, who is engaged in money laundering or terrorist financing, and

(d) where the financial services business has doubts about the veracity or adequacy of previously obtained identification data.

(3) The steps referred to in paragraph (1) are that -

(a) the customer shall be identified and his identity verified using identification data,

(b) any person purporting to act on behalf of the customer shall be identified and his identity and his authority to so act shall be verified,

(c) the beneficial owner and underlying principal shall be identified and reasonable measures shall be taken to verify such identity using identification data and such measures shall include, in the case of a legal person or legal arrangement, measures to understand the ownership and control structure of the customer,

(d) a determination shall be made as to whether the customer is acting on behalf of another person and, if the customer is so acting, reasonable measures shall be taken to obtain sufficient identification data to identify and verify the identity of that other person,

(e) information shall be obtained on the purpose and intended nature of each business relationship, and

(f) a determination shall be made as to whether the customer, beneficial owner and any underlying principal is a politically exposed person.

(4) A financial services business must have regard to any relevant rules and guidance in the Handbook in determining, for the purposes of this regulation and regulation 5, what constitutes reasonable measures.

Regulation 7

7.(1) Identification and verification of the identity of any person or legal arrangement pursuant to regulations 4 to 6 must, subject to paragraph (2) and regulation 4(1)(b), be carried out before or during the course of establishing a business relationship or before carrying out an occasional transaction.

(2) Verification of the identity of the customer and of any beneficial owners and underlying principals may be completed following the establishment of a business relationship provided that –

(a) it is completed as soon as reasonably practicable thereafter,

(b) the need to do so is essential not to interrupt the normal conduct of business,

and

(c) appropriate and effective policies, procedures and controls are in place which operate so as to manage risk.

Regulation 9

9. Where a financial services business can not comply with any of regulation 4(3)(a) to (d) it must -

(a) in the case of an existing business relationship, terminate that business relationship,

(b) in the case of a proposed business relationship or occasional transaction, not enter into that business relationship or carry out that occasional transaction with the customer, and

(c) consider whether a disclosure must be made pursuant to Part I of the Disclosure Law or section 15 or 15A of the Terrorism Law.

Regulation 10

10.(1) In the circumstances set out in paragraph (2), a financial services business may accept a written confirmation of identity and other matters from an introducer in relation to the requirements of regulation 4(3)(a) to (e) provided that -

(a) the financial services business also requires copies of identification data and any other relevant documentation to be made available by the introducer to the financial services business upon request and without delay, and

(b) the introducer keeps such identification data and documents.

(2) The circumstances referred to in paragraph (1) are that the introducer -

(a) is an Appendix C business, or

(b) is either an overseas branch of, or a member of the same group of bodies corporate as, the financial services business with which it is entering into the business relationship ("**receiving financial services business**"), and -

(i) the ultimate parent body corporate of the group of bodies corporate of which both the introducer and the receiving financial services business are members, falls within paragraph (2)(a),

(ii) the conduct of the introducer 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 on Money Laundering in respect of such a business, and

(iii) the conduct of which is supervised for compliance with the requirements referred to in subparagraph (ii), by the Commission or an overseas regulatory authority.

(3) Notwithstanding paragraph (1), where reliance is placed upon the introducer the responsibility for complying with the relevant provisions of regulation 4 remains with the receiving financial services business.

4 CUSTOMER DUE DILIGENCE

A financial services business must comply with the Rules in addition to the Regulations. The Rules are boxed and shaded for ease of reference. A financial services business should note that the Court must take account of the Rules and Guidance issued by the Commission in considering compliance with the Regulations.

4.1 Objectives

73. This chapter sets out the rules and provides guidance in respect of the CDD procedures to be undertaken by a financial services business in order to meet the CDD requirements of the Regulations in circumstances where the risk of a particular business relationship or occasional transaction has been assessed as normal. See chapter 17 for the definition of CDD.

74. Where the risk of a particular business relationship or occasional transaction has been assessed as higher than normal (described in this Handbook as high risk), the CDD requirements described in this chapter must be read in conjunction with the enhanced CDD requirements described in chapter 5 which deals with high risk relationships.

75. Where the risk of a particular business relationship or occasional transaction has been assessed as lower than normal (described in this Handbook as low risk), the CDD requirements described in this chapter should be read in conjunction with the requirements of chapter 6 which provides for circumstances in which reduced or simplified CDD policies, procedures and controls may be applied.

4.2 Customer Due Diligence – Policies, Procedures and Controls

76. Sound CDD procedures are vital for all financial services businesses because they:

- constitute an essential part of risk management, for example, by providing the basis for identifying, assessing, mitigating and managing risk;
- help to protect the financial services business and the integrity of the financial sector in which it operates by reducing the likelihood of a financial services business becoming a vehicle for, or a victim of, financial crime and terrorist financing;
- help the financial services business, at the time the CDD is carried out, to take comfort that the customers and other parties included in a business relationship are who they say they are, and that it is appropriate to provide them with the product or service requested; and
- help the financial services business 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 persons involved in a business relationship may be carrying out money laundering or terrorist financing.

4.3 Obligation to Identify and Verify Identity

77. Establishing that any customer, beneficial owner or underlying principal is the person that he claims to be is a combination of being satisfied that:

- a person exists – on the basis of appropriate identification data; and
- the customer, beneficial owner or underlying principal, is that person – by verifying from identification data, satisfactory confirmatory evidence of appropriate components of their identity.

78. A financial services business 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 assessed risk of the business relationship and occasional transaction.

79. The policies, procedures and controls must:

- be risk-based to differentiate between what is expected in low risk situations and what is expected in high risk situations and what is expected in situations which are neither high nor low risk;
- impose the least necessary burden on customers, beneficial owners and underlying principals consistent with meeting the requirements of the Regulations and Rules;
- not constrain access to financial services, for example, by those without driving licences or passports; and
- deal sensibly and sensitively with special groups for whom special processes may be appropriate, for example, the elderly and students studying overseas.

80. Financial services businesses must judge, on a risk-based approach, 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.

81. For customers that are legal persons or legal arrangements, the financial services business must:

(i) verify the legal status of the legal person or legal arrangement; and

(ii) obtain information concerning the customer's name, the names of trustees (for trusts), legal form, address, directors (for legal persons), foundation officials (for foundations) and provisions regulating the power to bind the legal person or arrangement.

82. Where the individual (or business relationship to which he is connected) presents a high risk, a financial services business must consider whether additional verification checks are necessary – see chapter 5 on high risk relationships.

4.4 Identification and Verification of Customers who are Individuals

83. Sections 4.4 to 4.9 of this chapter provide rules and guidance on how to meet the identification and verification of identity requirements of Regulation

84. Identification and verification of identity of a personal customer is a two-part process. The customer first identifies himself to the financial services business, by supplying a range of personal information. Generally, this information will be provided on some type of application form and the information requested may be used for business purposes over and above verifying the identity of the customer. The second part – the verification – consists of the financial services business verifying some or all of this information through the use of identification data.

85. For business relationships or occasional transactions which have been identified as low risk see chapter 6.

4.4.1 Identification data for individuals

86. A financial services business must, subject to section 6.2.1, collect relevant identification data on an individual, which includes:
    - legal name, any former names (such as maiden name) and any other names used;
    - principal residential address;
    - date and place of birth;
    - nationality;
    - any occupation, public position held and, where appropriate, the name of the employer; and
    - an official personal identification number or other unique identifier contained in an unexpired official document (for example, passport, identification card, residence permit, social security records, driving licence) that bears a photograph of the customer.

4.4.2 Verification of identity – the individual

87. The legal name, address, date and place of birth and nationality of the individual must be verified.

88. In order to verify the legal name, date and place of birth and nationality of the individual, the following documents are considered to be the best possible, in descending order of acceptability:

    - current passport (providing photographic evidence of identity);
    - current national identity card (providing photographic evidence of identity);
    - armed forces identity card.

89. The examples quoted above are not the only possibilities. There may be other documents of an equivalent nature which may be produced as satisfactory evidence of identity of the individual.

4.4.3 Verification of identity – the address

90. The following are considered to be suitable to verify the residential address of individuals:

- a bank/credit card statement or utility bill;
- correspondence from an independent source such as a central or local government department or agency (in Guernsey and Jersey this will include States departments, and parish authorities);
- commercial or electronic databases;
- a letter of introduction from an Appendix C business (see the definition in Appendix C to the Handbook) with which the individual has an existing business relationship and which confirms residential address;
- written communication from an Appendix C business (see the definition in Appendix C to the Handbook) in connection with a product or service purchased by the individual;
- lawyer's confirmation of property purchase, or legal document recognising title to property (low risk relationships and transactions only);
- a personal visit to the residential address; and
- an electoral roll.

91. For Guernsey residents and overseas residents who may encounter difficulties in providing evidence of their residential address, additional documents are listed in sections 4.4.4 and 4.5.3 respectively.

92. Identification data does not have to be in paper form. As well as documentary forms of verification, external electronic databases and other sources such as the internet, information published by government departments and law enforcement authorities, and subscription databases are accessible directly by financial services businesses. The evidential value of electronic checks should depend on the assessed risk of the business relationship or occasional transaction.

93. Where a financial services business is not familiar with the form of the evidence of identification data, it should take reasonable measures to satisfy itself that the evidence is genuine.

94. All key documents (or parts thereof) must be understood by an employee of the financial services business, and must be translated into English at the reasonable request of the FIS or the Commission.

95. Where establishing a face-to-face business relationship with or undertaking an occasional transaction for a customer who is an individual, reduced or simplified CDD may be carried out as set out in Regulation 6 – see chapter 6.

4.4.4 Guarding against the financial exclusion of Guernsey residents

96. Certain individuals may encounter difficulties in providing evidence of their Guernsey residential address using the sources identified above. Examples of such individuals include:

- seasonal workers who do not have a permanent residential address in Guernsey;
- individuals living in Guernsey in accommodation provided by their employer, with family (for example, in the case of minors), or in care homes, who may not pay directly for utility services; or
- Guernsey students living in university, college, school, or shared accommodation, who may not pay directly for utility services.

97. Where an individual has a valid reason for being unable to produce the requested documentation, and who would otherwise be excluded from accessing financial services and products, identification procedures should provide for alternative means of verifying an individual's Guernsey residential address. The following are examples of alternative methods of verifying identity:

- a letter from the head of the household at which the individual resides confirming that the applicant lives at that Guernsey address, setting out the relationship between the applicant and the head of the household, together with evidence that the head of the household resides at the address;
- a letter from the residential home or care home confirming residence of the applicant;
- a certificate of lawful residence or a Housing Licence;
- a letter from a director or manager of the Guernsey employer that confirms residence at a stated Guernsey address, and indicates 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, if possible, also verified; or
- in the case of a Guernsey student, a letter from a Guernsey resident parent or a copy of the acceptance letter for a place at the college/university. The student's residential address in Guernsey should also be obtained and, if possible, also verified.

4.5 Non Resident Individual Customers

98. In order to meet the requirements of Regulation 5 a financial services business must take adequate measures to manage and mitigate the specific risks of business relationships or occasional transactions with a customer who is not a Guernsey resident.

99. See Sections 6.2.1 and 6.2.2 for information on the provisions applicable to Guernsey residents who meet the criteria for reduced or simplified CDD measures to be applied.

4.5.1 Adequate measures

100. A financial services business must ensure that it takes adequate measures which include one or more of the following:

- requiring additional documents to complement those which are required for face-to-face customers;

- development of independent contact with the customer and other third parties responsible for the source of funds or company registrations, etc.;
- third party introduction; or
- requiring the first payment to be carried out through an account in the customer's name with a bank situated in a country or territory listed in Appendix C to the Handbook.

101. In addition, where copy documentation is provided, a financial services business must ensure that the copy documents have been certified by a suitable certifier.

4.5.2 Suitable certifiers

102. Use of a certifier guards against the risk that identification data provided does not correspond to the individual whose identity is to be verified. For certification to be effective, the certifier will need to have seen the original documentation and, where certifying evidence of identity containing a photograph, have met the individual in person..

103. A financial services business must give consideration to the suitability of a certifier based on the assessed risk of the business relationship or occasional transaction, together with the level of reliance being placed on the certified documents. The financial services business must exercise caution when considering certified copy documents, especially where such documents originate from a country or territory perceived by the financial services business to represent a high risk, or from unregulated entities in any country or territory.

104. Where certified copy documents are accepted, the financial services business must satisfy itself, where possible, that the certifier is appropriate, for example, by satisfying itself that the certifier is not closely related to the person whose identity is being certified.

105. A suitable certifier must certify that he has seen original documentation verifying identity and residential address.

106. The certifier must also sign and date the copy identification data and provide adequate information so that contact can be made with the certifier in the event of a query.

4.5.3 Verification of residential address of overseas residents

107. There may be occasions when an individual resident abroad is unable to provide evidence of his residential address using the means set out in section 4.4.3. Examples of such individuals include residents of countries without postal deliveries and no street addresses, who rely on post office boxes or employers for delivery of mail.

108. Where 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 with the financial services business, satisfactory verification of address may be established by:

- 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
- any of the means provided in sections 4.4.3 and 6.2.2 without regard to any restrictions imposed on such documents.

4.6 Identification and Verification of Customers who are not Individuals

109. The identification and verification requirements in respect of customers who are not individuals are different from those for individuals, as beneficial owners and underlying principals must also be identified. Although a customer who is not an individual has a legal status which can be verified, each customer also involves a number of individuals, whether as beneficial owners (or equivalent), directors (or equivalent) or underlying principals, who have the power to direct movement of the customer's funds or assets.

110. As identified in the following paragraphs, certain information about the customer must be obtained as a minimum requirement. In addition, on the basis of the assessed money laundering and terrorist financing risk of the particular customer/product/service combination, a financial services business must consider how the identity of the customer and of specific individuals must be verified, and what additional information in respect of the entity must be obtained.

4.6.1 Legal bodies

111. Legal body refers to bodies corporate, partnerships, associations or other bodies which are not natural persons or legal arrangements. Foundation relationships are dealt with separately – see sections 4.6.2 to 4.6.3. Trust relationships and other legal arrangements are also dealt with separately – see sections 4.6.4 to 4.6.6.

112. Where a legal body is either a collective investment scheme regulated by the Commission or a legal body quoted on a regulated market or is a subsidiary of such, then a financial services business may consider the legal body to be the principal to be identified and verified - see section 6.2.3.

113. Where a legal body which is not either a collective investment scheme regulated by the Commission or a legal body quoted on a regulated market is the customer, beneficial owner or underlying principal a financial services business must:

- identify and verify the identity of the legal body. The identity includes name, any official identification number, date and country or territory of incorporation if applicable;
- identify and verify any registered office address and principal place of business (where different from registered office) where the risk presented by

the legal body is other than low;

- identify and verify the individuals ultimately holding a 25% or more interest in the capital or net assets of the legal body;
- identify and verify the individuals, including beneficial owners, underlying principals, directors, authorised signatories or equivalent, with ultimate effective control over the capital or assets of the legal body; and
- verify the legal status of the legal body.

114. When seeking to identify and verify the identity of beneficial owners, underlying principals, the directors and authorised signatories or equivalent in accordance with this section, reference should be made to the identification and verification requirements for personal customers – see sections 4.3, 4.4 and 4.5. It may be appropriate to consider directors with ultimate effective control as being those who have authority to operate an account or to give the financial services business instructions concerning the use or transfer of funds or assets.

115. One or more of the following examples are considered suitable to verify the legal status of the legal body:

- a copy of the Certificate of Incorporation (or equivalent) if applicable;
- a company registry search, if applicable, including confirmation that the legal body has not been, and is not in the process of being, dissolved, struck off, wound up or terminated;
- a copy of the latest audited financial statements;
- a copy of the Memorandum and Articles of Association or equivalent constitutional documentation;
- a copy of the Directors' Register;
- a copy of the Shareholders' Register;
- independent information sources, including electronic sources, for example, business information services;
- a copy of the Board Resolution authorising the opening of the account and recording account signatories; and
- a personal visit to the principal place of business.

116. Where the documents provided are copies of the originals the financial services business must ensure they are certified by the company secretary, director, manager or equivalent officer or by a suitable certifier.

117. Where the legal body (or any beneficial owner or underlying principal connected with the legal body) presents a high risk, a financial services business must consider whether additional verification checks are appropriate, for example, obtaining additional information or documentation.

118. A general threshold of 25% is deemed to indicate effective control or ownership. Individuals having ultimate effective control over a legal body will often include directors or equivalent. In the case of partnerships, associations, clubs, societies, charities, church bodies, institutes, mutual and friendly societies, cooperative 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 of a foundation and any supervisors.

119. Powers of attorney and similar third party mandates must be given particular attention if there is no evident reason for granting them. In addition, an unnecessarily wide-ranging scope to the mandate must also be given particular attention. In any case, a financial services business must obtain a copy of the power of attorney (or other authority or mandate) that provides the individuals representing the legal body with the right to act on its behalf and verification must be undertaken on the holders of the powers of attorney as well as the customer. A financial services business must also ascertain the reason for the granting of the power of attorney.

4.6.2 Obligations of financial services businesses establishing or administering foundations

120. When establishing or administering a foundation relationship, a financial services business must, in order to identify and verify the identity of its customer and any beneficial owner and underlying principal, identify:

- the founder(s);
- all councillors;
- any guardian;
- any beneficiary including any default recipient; and
- any other person with ultimate effective control over the assets of the foundation.

121. Subject to paragraph 122 verification of the identity of beneficiaries must, be undertaken prior to any distribution of foundation funds to (or on behalf of) that beneficiary in accordance with the requirements of Regulation 7.

122. Where a business relationship has been assessed as a high risk relationship, verification of the identity of any beneficiaries must, where possible, be undertaken at the time that the assessment of risk is made. Where it is not possible to do so, (for example, because they are disenfranchised) the reasons must be documented.

123. Verification of the identity of other underlying principals such as founders, councillors, guardians and any other persons with ultimate effective control must be carried out before or during the course of establishing the business relationship.

4.6.3 Obligations of financial services businesses dealing with foundations

124. Subject to section 6.5 of the Handbook, a financial services business entering into a relationship with a customer which is a foundation must:

- identify and verify the identity of the foundation. The identity includes name, any official identification number, date and country or territory of registration if applicable;
- identify and verify any registered office address and principal place of operation/administration (where different from the registered office);
- identify and verify the identity of any registered agent of the foundation unless they themselves are either subject to the Handbook or are an Appendix C business (see the definition in Appendix C to the Handbook);
- verify the legal status of the foundation;
- require the registered agent, foundation officials or other relevant person to identify and notify it of the names of the underlying principals and beneficial owners, i.e:
    - the founder(s);
    - all councillors;
    - any guardian;
    - any beneficiary including any default recipient; and
    - any other person with ultimate effective control over the capital or assets of the legal body; and
- understand the nature of the foundation structure and the nature and purpose of activities undertaken by the structure sufficient to monitor such activities and to fully understand the business relationship.

125. Subject to paragraph 126 verification of the identity of beneficiaries must be undertaken prior to any distribution of foundation assets to (or on behalf of) that beneficiary in accordance with the requirements of Regulation 7.

126. Where a business relationship has been assessed, as a high risk relationship, verification of the identity of any beneficiaries must, where possible, be undertaken at the time that the assessment of risk is made. Where it is not possible to do so, (for example, because they are disenfranchised) the reasons must be documented.

127. Verification of the identity of the underlying principals and beneficial owners must be undertaken either by the financial services business itself or, provided that the rules in section 4.10 of the Handbook are met, by requesting the registered agent, where one has been appointed, to provide identification data on them, by way of a certificate or summary sheet (see Appendix B for an example).

128. When identifying and verifying the identity of founders, foundation officials, beneficiaries and others in accordance with this section, financial services businesses must act in accordance with the identification and verification

requirements for customers who are individuals and legal bodies – see sections 4.4 and 4.6.1.

129. One or more of the following examples are considered suitable to verify the legal status of the foundation:

- a copy of the Certificate of Registration;
- 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;
- a copy of the latest audited financial statements;
- a copy of the Charter; and
- a copy of the Council Resolution authorising the opening of the account and recording account signatories.

130. Where the documents provided are copies of the originals the financial services business must ensure they are certified by a foundation official or by a suitable certifier.

131. Powers of attorney and similar third party mandates must be given particular attention if there is no evident reason for granting them. In addition, an unnecessarily wide-ranging scope to the mandate must also be given particular attention. In any case, a financial services business must obtain a copy of the power of attorney (or other authority or mandate) that provides the individuals representing the foundation with the right to act on its behalf and verification must be undertaken on the holders of the powers of attorney as well as the customer. A financial services business must also ascertain the reason for the granting of the power of attorney.

4.6.4 Legal arrangements

132. There is a wide variety of trusts and other legal 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.

133. Trusts 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 customer.

4.6.5 Obligations of trustees

134. When establishing a trust relationship, a financial services business which is acting as a trustee must, in order to identify and verify the identity of its customer and any beneficial owner and underlying principal, identify:

- the settlor(s);

- any protector(s) or co-trustee(s); and
- any beneficiary with a vested interest or any person who is the object of a power.

135. Subject to paragraph 136 verification of the identity of beneficiaries with a vested interest or any person who is the object of a power must be undertaken prior to any distribution of trust assets to (or on behalf of) that beneficiary or person in accordance with the requirements of Regulation 7.

136. Where a business relationship has been assessed as a high risk relationship, verification of the identity of any beneficiaries must, where possible, be undertaken at the time that the assessment of risk is made. Where it is not possible to do so, the reasons must be documented.

137. The verification of identity of other underlying principals such as settlors, co-trustees and protectors must be carried out before or during the course of establishing a business relationship.

138. When identifying and verifying the identities of beneficiaries and others in accordance with this section, trustees must act in accordance with the identification and verification requirements for personal customers and legal bodies – see sections 4.4 and 4.6.1.

4.6.6 Obligations of financial services businesses dealing with trusts

139. Subject to section 6.5 of the Handbook, a financial services business entering a relationship with a customer which is a trust must:

- verify the legal status and the name and date of establishment of the trust;
- verify the identity of the trustees of the trust unless they are themselves subject either to the Handbook or are an Appendix C business (see the definition in Appendix C to the Handbook);
- require the trustee of the trust to identify and notify it of the names of the underlying principals and beneficial owners, i.e.:
    - the settlor(s) (the initial settlor(s) and any persons subsequently settling funds into the trust);
    - any protector(s) or trustee(s); and
    - any beneficiary with a vested interest or any person who is the object of a power; and
- understand the nature of the trust structure and the nature and purpose of activities undertaken by the structure sufficient to monitor such activities and to fully understand the business relationship.

140. Verification of the identity of the underlying principals and beneficial owners must be undertaken either by the financial services business itself or, provided that the rules in section 4.10 of the Handbook are met, by requesting the trustee to provide identification data on them, by way of a certificate or summary sheet (see

Appendix B for an example).

141. Subject to paragraph 142 verification of the identity of beneficiaries or any persons who are the object of a power must be undertaken prior to any distribution of trust assets to (or on behalf of) that beneficiary in accordance with the requirements of Regulation 7.

142. Where a business relationship has been assessed as a high risk relationship, verification of the identity of any beneficiaries must, where possible, be undertaken at the time that the assessment of risk is made. Where it is not possible to do so, the reasons must be documented.

143. When identifying and verifying the identity of trustees, beneficiaries and others in accordance with this section, financial services businesses must act in accordance with the identification and verification requirements for customers who are individuals and legal bodies – see sections 4.4 and 4.6.1.

4.7 Employee benefit schemes, share option plans or pension schemes

144. Where the product or service is:

- an employee benefit scheme or arrangement;
- an employee share option plan;
- a pension scheme or arrangement
- a superannuation scheme; or
- a similar scheme 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, for example, the administrator or the scheme manager is considered as the principal and must be identified and verified in accordance with the requirements of this chapter.

145. In these types of relationships, the financial services business should consider the person providing the source of funds as a factor when determining the risk classification to be given to the relationship.

4.8 Life and Other Investment Linked Insurance

146. Where the product or service is a life or other investment linked insurance policy, the issuer, in order to meet the requirements of Regulation 4, must, in addition to identifying and verifying the customer and beneficial owner also identify and verify the identity of any beneficiaries..

147. Verification of the identity of beneficiaries must be undertaken prior to any distribution to (or on behalf of) those beneficiaries.

4.9 Acquisition of a Business or Block of Customers

148. There are circumstances where a financial services business may acquire a business with established business relationships or a block of customers, for example, by way of asset purchase.

149. Before taking on this type of business, in order to avoid breaching the Regulations, a financial services business should undertake enquiries on the vendor sufficient to establish the level and the appropriateness of identification data held in relation to the customers and the business relationships of the business to be acquired.

150. A financial services business may consider it appropriate to rely on the information and documentation previously obtained by the vendor where the following criteria are met:

- the vendor is an Appendix C business (see the definition in Appendix C to the Handbook);
- the financial services business has assessed that the CDD policies, procedures and controls operated by the vendor were satisfactory; and
- the financial services business has obtained from the vendor, identification data for each customer acquired.

151. Where deficiencies in the identification data held are identified (either at the time of transfer or subsequently), the accepting financial services business must determine and implement a programme to remedy any such deficiencies.

4.10 Customer Due Diligence Procedures for Introduced Business Relationships

152. An introduced business relationship is where a financial services business, lawyer or accountant is acting on behalf of one or more third parties who are also its customers and establishes a business relationship on their behalf with a financial services business. Introducer relationships may be business relationships on behalf of a single third party or on behalf of more than one third party, including a pool of such persons.

153. A business relationship established by an introducer on behalf of more than one of its customers is described by the Handbook as a pooled relationship – see section 4.12.

154. It is important to distinguish between introduced business relationships and intermediary business relationships. In the latter relationships, an intermediary meeting the criteria necessary to be considered as such can be treated as the customer – see section 6.5.

155. Regulation 10 provides for the circumstances in which a financial services business may place reliance on an introducer to have verified the identity of the customer, beneficial owners and any underlying principals.

156. When establishing an introducer relationship a financial services business must satisfy itself that the introducer:

- has appropriate risk-grading procedures in place to differentiate between the CDD requirements for high and low risk relationships; and
- conducts appropriate and effective CDD procedures in respect of its customers, including enhanced CDD measures for PEP and other high risk relationships.

157. In the circumstances set out in Regulation 10, a financial services business relying upon a third party must immediately obtain written confirmation of identity from the introducer, by way of a certificate or summary sheet(s), detailing elements (a) – (d) of the CDD process (see below).

158. A financial services business 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.

159. The CDD process referred to above in accordance with Regulation 4(3) includes the following elements:

(a) identifying the customer by name and verifying that customer's identity using identification data;

(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 financial institution is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements this includes financial institutions taking reasonable measures to understand the ownership and control structure of the customer;

(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) obtaining information on the purpose and intended nature of the business relationship.

160. A financial services business must recognise that introduced business by its very nature, for example, relying on a third party, has the capacity to be high risk and a financial services business must use a risk-based approach when deciding whether it is appropriate to rely on a certificate or summary sheet from an introducer in accordance with Regulation 10 or whether it considers it necessary to do more.

161. A financial services business must have a programme of testing to ensure that introducers are able to fulfil the requirement that certified copies or originals of the identification data will be provided upon request and without delay. This will involve financial services businesses adopting ongoing procedures to ensure they have the means to obtain that identification data and documentation.

162. In accordance with the Regulations the ultimate responsibility for customer identification and verification will remain, as always, with the financial services business relying on the introducer.

163. A template certificate which may be used by financial services businesses for introduced business is contained within Appendix A.

4.10.1 Group introducers

164. Where a customer is introduced by one part of a financial services group to another, it is not necessary for his identity to be re-verified, provided that:

- the requirements of Regulation 10 are satisfied;
- as a minimum, the financial services business receives a written confirmation from the group introducer in accordance with the requirements for introduced business as detailed in section 4.10 above;
- the financial services business takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available upon request without delay. This requirement would be satisfied if the financial services business has access to the information electronically on the group's database.

165. Group introduced business must not be regarded as intrinsically low risk. As identified in section 4.10 a financial services business must use a risk-based approach when deciding whether it is appropriate to rely on a certificate or summary sheet from a group introducer or whether it considers it necessary to do more bearing in mind that, ultimately, the responsibility for customer identification and verification will remain, as always, with the financial services business relying on the introducer.

4.11 Chains of Introducers

166. Sections 4.10, 4.10.1 provide for a financial services business to rely on a certificate or summary sheet from an introducer which has provided an assurance that the introducer retains the verification documentation and other evidence collected under the CDD process.

167. Chains of introducers are not permitted, a financial services business must not place reliance on an introducer who forms part of a chain. This avoids a situation whereby, should the middle institution fall away, the receiving financial services 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.

4.12 Pooled Bank Accounts

168. Banks often hold pooled accounts on behalf of professional firms and financial services businesses. These accounts contain the funds of more than one client. Where the requirement is for the pooled account to be held on an undisclosed

basis, section 6.5 provides information on the CDD requirements of such relationships.

169. Where the pooled account is held on behalf of a professional firm or a financial services business which:

- does not meet the requirements as set out in section 6.5.1; and
- the product or service is not a product or service set out in section 6.5.2,

then the bank must identify and verify the identity of the customers, beneficial owners and underlying principals for whom the professional firm or financial services business is acting in accordance with the requirements of chapter 4 of the Handbook.

4.13 Timing of Identification and Verification of Identity

170. Regulation 7 prescribes the timing for identification and verification of identity.

171. When the circumstances are such that verification of identity of customers, beneficial owners and underlying principals may be completed following the establishment of the business relationship or after carrying out the occasional transaction, a financial services business must have appropriate and effective policies, procedures and controls in place so as to manage the risk which must include:

- establishing that it is not a high risk relationship;
- monitoring by senior management of these business relationships to ensure verification of identity is completed as soon as reasonably practicable;
- ensuring funds received are not passed to third parties; and
- establishing procedures to limit the number, types and/or amount of transactions that can be undertaken.

172. A financial services business 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 such circumstances a financial services business should refer to section 4.14 of the Handbook.

4.13.1 Occasional transactions

173. If identity is known, verification of identity is not required in the case of occasional transactions (whether single or linked), below the threshold in the Regulations, 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.

4.14 Failure to Complete Customer Due Diligence Procedures

174. When a financial services business has been unable, within a reasonable time frame, to complete CDD procedures in accordance with the requirements of the Regulations and the Handbook it must assess the circumstances and ensure that the appropriate action is undertaken as required by Regulation 9.

175. 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 financial services business. In such circumstances a financial services business must ensure that the risk is managed and mitigated effectively until such time as termination of the relationship is possible.

176. A financial services business must ensure that where funds have already been received, they are returned to the source from which they were originally received (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.

CHAPTER 5 – HIGH RISK RELATIONSHIPS

Key Regulations

Sections in this Chapter

REGULATIONS

The requirements of the Regulations to which the rules and guidance in this chapter particularly relate are:

- Regulation 3, which provides for a financial services business to identify and assess the risks of money laundering and terrorist financing and to ensure that its policies, procedures and controls are effective and appropriate to the assessed risk. See chapter 3.
- Regulation 4, which provides for the required customer due diligence measures, when they should be applied and to whom they should be applied. See chapter 4.
- Regulation 5, which provides for enhanced customer due diligence measures in respect of business relationships and occasional transactions which are identified as high risk. See below.
- Regulation 8, which makes provisions in relation to anonymous accounts and shell banks. See chapter 8.
- Regulation 15, which makes provisions in relation to the review of compliance. See chapter 2.

Regulation 5

5.(1) Where a financial services business is required to carry out customer due diligence, it must also carry out enhanced customer due diligence in relation to the following business relationships or occasional transactions –

(a) a business relationship or occasional transaction in which the customer or any beneficial owner or underlying principal is a politically exposed person,

(b) a business relationship which is -

(i) a correspondent banking relationship, or

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

(c) a business relationship or an occasional transaction -

(i) where the customer is established or situated in a country or territory that does not apply or insufficiently applies the Financial Action Task Force Recommendations on Money Laundering, or

(ii) which the financial services business considers to be a high risk relationship, taking into account any notices, instructions or warnings issued from time to time by the Commission, and

(d) a business relationship or an occasional transaction which has been assessed as a high risk relationship pursuant to regulation 3(2)(a).

(2) In paragraph (1) -

(a) "**enhanced customer due diligence**" means -

(i) obtaining senior management approval for establishing a business relationship or undertaking an occasional transaction;

(ii) obtaining senior management approval for, in the case of an existing business relationship with a PEP, continuing that relationship;

(iii) taking reasonable measures to establish the source of any funds and of the wealth of the customer and beneficial owner and underlying principal;

(iv) carrying out more frequent and more extensive ongoing monitoring in accordance with regulation 11; and

(v) taking one or more of the following steps as would be appropriate to the particular business relationship or occasional transaction-

(A) obtaining additional identification data;

(B) verifying additional aspects of the customer's identity; and

(C) obtaining additional information to understand the purpose and intended nature of each business relationship.

(b) "**politically exposed person**" means -

(i) 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 including, without limitation -

(A) heads of state or heads of government,

(B) senior politicians and other important officials of political parties,

(C) senior government officials,

(D) senior members of the judiciary,

(E) senior military officers, and

(F) senior executives of state owned body corporates,

(ii) an immediate family member of such a person including, without limitation, a spouse, partner, parent, child, sibling, parent-in-law or grandchild of such a person and in this subparagraph "**partner**" means a person who is considered by the law of the country or territory in which the relevant public function is held as being equivalent to a spouse, or

(iii) a close associate of such a person, including, without limitation -

(A) a person who is widely known to maintain a close business relationship with such a person, or

(B) a person who is in a position to conduct substantial financial transactions on behalf of such a person.

(4) Where the customer was not a Guernsey resident when a financial services business carried out an activity set out in regulation 4(2)(a) or (b), a financial services business must take adequate measures to compensate for the specific risk arising as a result -

(a) when carrying out customer due diligence, and

(b) where the activity was establishing a business relationship, when carrying out monitoring of that relationship pursuant to regulation 11.

5 HIGH RISK RELATIONSHIPS

A financial services business must comply with the Rules in addition to the Regulations. The Rules are boxed and shaded for ease of reference. A financial services business should note that the Court must take account of the Rules and Guidance issued by the Commission in considering compliance with the Regulations.

5.1 Objectives

177. This chapter provides for the treatment of business relationships and occasional transactions which have been assessed as high risk and should be read in conjunction with chapter 3 of the Handbook, which provides guidance on the assessment of risk and with chapter 4 which provides for the standard CDD requirements.

5.2 Enhanced Policies, Procedures and Controls

178. Where a financial services business has assessed, taking into account the high risk indicators provided in chapter 3, that the business relationship or occasional transaction is a high risk relationship – whether because of the nature of the customer, the business relationship, or its location, or because of the delivery channel or the product/service features available – the financial services business must ensure that its policies, procedures and controls require enhanced CDD measures to be undertaken as required in Regulation 5.

5.3 Politically Exposed Persons

179. As required by Regulation 4 when carrying out CDD a determination must be made by the financial services business as to whether the customer, beneficial owner and any underlying principal is a PEP.

180. Where a financial services business has determined that the business relationship or occasional transaction is one where the customer or any beneficial owner or underlying principal is a PEP, the financial services business must ensure that it has appropriate and effective policies, procedures and controls in place to ensure compliance with the enhanced due diligence requirements of Regulation 5.

181. In order to determine whether a customer, beneficial owner or underlying principal is a PEP, a financial services business must consider:

- assessing countries which pose the highest risk of corruption – one source of information is the Transparency International Corruption Perception Index;
- establishing 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 customers, beneficial owners or underlying principals have any connections with such individuals – the UN, the European Parliament, the UK Foreign and Commonwealth Office, the

Group of States Against Corruption may be useful information sources; and
- using commercially available databases.

Website addresses for the above authorities and other useful website links are provided in Appendix I.

5.3.1 Source of funds and source of wealth

182. The source of funds refers to the activity which generates the 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.

183. Understanding the customer's source of funds and source of wealth are important aspects of CDD especially in relationships with PEPs.

184. A financial services business must, in establishing the source of any funds or wealth, consider and document its 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.

5.4 Correspondent Relationships

185. Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Used by banks throughout the world, correspondent accounts enable banks to conduct business and provide services that the bank does not offer directly. There are similar relationships in other areas of financial services.

186. In relation to correspondent relationships for banking and those established for securities transactions or funds transfers, whether for the financial services business as principal or for its customers, a financial services business must take additional steps in relation to CDD including those in the bullets below and (where relevant) those in the following paragraph:

- gather sufficient information about a respondent institution to understand fully the nature of the respondent's business;
- determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;
- assess the respondent institution's AML/CFT policies, procedures and controls, and ascertaining that they are adequate, appropriate and effective;
- obtain board or senior management approval, i.e. sign off before establishing new correspondent relationships; and
- document the respective AML/CFT responsibilities of each institution.

187. Where a correspondent relationship involves the maintenance of "payable-

through accounts", a financial services business must also take steps so that they are satisfied that:

- their customer (the "respondent financial services business") has performed all the required CDD obligations set out in the Regulations and chapter 4 of the Handbook on those of its customers that have direct access to the accounts of the correspondent financial services business; and
- the respondent financial services business is able to provide relevant customer identification data upon request to the correspondent financial services business.

188. Financial services businesses must, pursuant to Regulation 15(a), ensure that appropriate and effective policies, procedures and controls are in place when establishing correspondent relationships with foreign banks and other institutions.

189. Additionally, a financial services business must have appropriate and effective policies, procedures and controls in place to ensure compliance with the requirements of Regulation 8 in respect of shell banks.

5.5 Countries or Territories that Do Not or Insufficiently Apply the FATF Recommendations and other High Risk Countries or Territories

190. In addition to the enhanced CDD measures required by Regulation 5 for high risk relationships, financial services businesses must give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries or territories that do not or insufficiently apply the FATF Recommendations and from other countries or territories closely associated with illegal drug production/processing or trafficking, corruption, terrorism, terrorist financing and other organised crime.

191. Financial services businesses must:

- ensure they are aware of concerns about weaknesses in the AML/CFT systems of other countries or territories;
- identify transactions which (in the context of business relationships and occasional transactions) have no apparent economic or visible lawful purpose and examine the background and purpose of such transactions; and
- record in writing the findings of such examinations in order to assist the Commission, the FIS, other domestic competent authorities and auditors.

192. When determining which countries or territories these policies, procedures and controls should apply to, a financial services business must consider:

- Business from Sensitive Sources Notices and Instructions issued from time to time by the Commission;
- findings of reports issued by the FATF, FATF-style regional bodies, FATF associate members such as Moneyval and Asia Pacific Group, the Offshore Group of Banking Supervisors, Transparency International, the International Monetary Fund and the World Bank;

- situations where the country or territory has not been the subject of an AML/CFT assessment; and
- 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.

5.6 Legal Persons able to Issue Bearer Instruments

193. As identified in section 3.5.3 of the Handbook, when assessing the risk of a particular relationship a financial services business must 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.

194. In circumstances where such a relationship has been identified, and in order to address the specific risks of such a relationship a financial services business must undertake enhanced CDD measures to ensure that the CDD requirements of Regulation 4 are met and that legal persons who have issued or have the potential to issue bearer shares, bearer warrants or bearer negotiable instruments are not misused for money laundering and/or terrorist financing.

CHAPTER 6 – LOW RISK RELATIONSHIPS

Key Regulations

Sections in this Chapter

REGULATIONS

The requirements of the Regulations to which the rules and guidance in this chapter particularly relate are:

- Regulation 3, which provides for a financial services business to identify and assess the risks of money laundering and terrorist financing and to ensure that its policies, procedures and controls are effective and appropriate to the assessed risk. See chapter 3.
- Regulation 4, which provides for the required customer due diligence measures, when they should be applied and to whom they should be applied. See chapter 4.
- Regulation 6, which provides for reduced or simplified customer due diligence measures to be applied to business relationships which have been identified as being low risk relationships. See below.
- Regulation 15, which makes provisions in relation to the review of compliance. See chapter 2.

Regulation 6

6.(1) Where a financial services business is required to carry out customer due diligence in relation to a business relationship or occasional transaction which has been assessed as a low risk relationship pursuant to regulation 3(2)(a), it may, subject to the following provisions of this regulation -

(a) apply reduced or simplified customer due diligence measures, or

(b) treat an intermediary as if it were the customer.

(2) The discretion in paragraph (1) may only be exercised in accordance with the requirements set out in chapter 6 of the Handbook.

(3) For the avoidance of doubt, the discretion in paragraph (1) shall not be exercised -

(a) where the financial services business knows or suspects or has reasonable grounds for knowing or suspecting that any party to a business relationship or any beneficial owner or underlying principal is engaged in money laundering or terrorist financing, or

(b) in relation to business relationships or occasional transactions where the risk is other than low.

6 LOW RISK RELATIONSHIPS

A financial services business must comply with the Rules in addition to the Regulations. The Rules are boxed and shaded for ease of reference. A financial services business should note that the Court must take account of the Rules and Guidance issued by the Commission in considering compliance with the Regulations.

6.1 Objectives

195. This chapter provides for the treatment of relationships and occasional transactions which have been assessed pursuant to Regulation 3 as low risk and should be read in conjunction with chapter 3 of the Handbook, which provides guidance on the assessment of risk and with chapter 4 which provides for the standard CDD requirements.

6.2 Simplified or Reduced CDD Measures

196. The general rule is that business relationships and occasional transactions are subject to the full range of CDD measures as identified in chapter 4 of the Handbook, including the requirement to identify and verify the identity of the customer, beneficial owners and any underlying principals. Nevertheless, there are circumstances where the risk of money laundering or terrorist financing has been assessed as being low (for example, a locally resident retail customer purchasing a low risk product where the purpose and intended nature of the business relationship or occasional transaction is clearly understood by the financial services business and where no aspect of the business relationship or occasional transaction is considered to carry a high risk of money laundering or terrorist financing), or where information on the identity of the customer, beneficial owners and underlying principals is publicly available, or where adequate checks and controls exist elsewhere in national systems.

197. In such circumstances a financial services business may consider applying simplified or reduced CDD measures when identifying and verifying the identity of the customer, beneficial owners and underlying principals.

198. A financial services business 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 CDD documentation and information held is undertaken to determine whether it remains appropriate to the revised risk of the business relationship or occasional transaction.

199. Where a financial services business has taken a decision to apply reduced or simplified CDD measures, documentary evidence must be retained which reflects the reason for the decision.

200. The possibility of applying simplified or reduced CDD measures does not remove from the financial services business its responsibility for ensuring that the level of CDD required is proportionate to the risk.

201. A financial services business must ensure that where the risk has been assessed as anything other than low that simplified or reduced CDD measures are not applied.

6.2.1 Identification data for Guernsey residents

202. Where establishing a business relationship with or undertaking an occasional transaction for an individual customer who is a Guernsey resident and the requirements for the application of simplified or reduced CDD measures, as set out above are met, a financial services business must obtain at a minimum the following information in relation to an individual customer:

- legal name, any former names (such as maiden name) and any other names used;
- principal residential address;
- date of birth; and
- nationality

6.2.2 Verification of identity for Guernsey residents

203. Subject to section 6.4 the legal name and either the principal residential address or the date of birth of the individual must be verified.

204. In order to verify the legal name and either the principal residential address or date of birth, any one of the following documents is considered to be appropriate:

- current passport (providing photographic evidence of identity);
- current national identity card (providing photographic evidence of identity);
- armed forces identity card;
- current driving licence incorporating photographic evidence of identity;
- birth certificate in conjunction with a verification document listed in section 4.4.3;
- independent data sources (including electronic sources).

205. When relying on independent data sources to verify identity a financial services business must 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 by the financial services business.

6.2.3 Legal bodies quoted on a regulated market

206. In order for a financial services business to consider the legal body as the principal to be identified, it must obtain documentation which confirms:

- the legal body is a collective investment scheme regulated by the

Commission; or

- the legal body is quoted on a regulated market (or is a wholly owned subsidiary of such a legal body); and

must identify and verify authorised signatories who have authority to operate an account or to give the financial services business instructions concerning the use or transfer of funds or assets.

207. For example, where a bank is opening an account for a collective investment scheme regulated by the Commission, the bank may treat the scheme itself as the customer to be identified and verified..

6.2.4 Appendix C business

208. When the customer has been identified as an Appendix C business (see the definition in Appendix C to the Handbook), and the purpose and intended nature of the relationship is understood, verification of the identity of the Appendix C business is not required. However, if the Appendix C business is acting for underlying principals then those underlying principals must be identified and their identity verified in accordance with the requirements of the Handbook.

209. Where a person authorised to act on behalf of a legal body or legal arrangement is acting in the course of employment by an Appendix C business (see definition in Appendix C to the Handbook), it is not necessary to identify and verify the identity of such persons. One such example would be a director (or equivalent) of a Guernsey fiduciary which is acting as trustee.

6.3 Non-Guernsey Collective Investment Funds

210. A Guernsey regulated financial services business which is providing services within the scope of a licence issued to it by the Commission, to a collective investment fund established outside Guernsey may, in certain circumstances, place reliance on a contracted party, for instance the administrator or the transfer agent, of the fund to have undertaken CDD procedures on the investor.

211. Where the financial services business in Guernsey wishes to rely on the CDD procedures of the administrator of the fund, the financial services business must:

- undertake CDD procedures in respect of the administrator to ensure that it is an Appendix C business and that it is regulated and supervised for investment business; and
- require the administrator to provide a written confirmation which:
    - contains adequate assurance that the administrator conducts the necessary CDD procedures in respect of investors in the fund;
    - confirms that the administrator has appropriate risk-grading procedures in place to differentiate between the CDD requirements for high and low risk relationships; and
    - contains an assurance that the administrator will notify the

financial services business of any investor in the fund categorised as a PEP.

In addition, the Guernsey financial services business must have a programme for testing and reviewing the CDD procedures of the administrator.

6.4 Receipt of Funds as Verification of Identity

212. Where the customer, beneficial owner and any underlying principal have been identified, the relationship or occasional transaction is considered to be a low risk relationship and the receipt of funds is considered to provide a satisfactory means of verifying identity, the financial services business must ensure that:

- all initial and future funds are received from an Appendix C business (see the definition in Appendix C to the Handbook);
- all initial and future funds come from an account in the sole or joint name of the customer or underlying principal;
- payments may only be paid to an account in the customer's name (i.e. no third party payments allowed);
- no payments may be received from third parties;
- no changes are made to the product or service that enable funds to be received from or paid to third parties; and
- no cash withdrawals are permitted other than by the customer or 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.

213. A financial services business must retain documentary evidence to demonstrate the reasonableness of its conclusion that the relationship being established or the occasional transaction being undertaken presents a low risk of money laundering and terrorist financing.

214. A financial services business must ensure that, once a relationship has been established, should any of the above conditions no longer be met then verification of identity is carried out in accordance with chapter 4 of the Handbook.

215. Should a financial services business have reason to suspect the motives behind a particular transaction or believe that the business is being structured to avoid the standard identification requirements, it must ensure that receipt of funds is not used to verify the identity of the customer, beneficial owner or underlying principal.

6.5 Intermediary Relationships

216. Section 4.10 of the Handbook provides for the identification and verification requirements in relation to introduced business relationships, i.e. where a financial services business enters into a business relationship on behalf of one or more third parties, who are its customers, with another financial services business.

217. Regulation 6 and sections 6.5.1 and 6.5.2 of the Handbook set out the criteria which must be met for an intermediary relationship to be established. In such circumstances, it will not be necessary to undertake CDD procedures on the intermediary's customers unless the financial services business considers this course of action to be appropriate.

218. Before establishing an intermediary relationship, the financial services business must undertake a risk assessment of the proposed business relationship. Such an assessment will allow the financial services business to consider whether it is appropriate to consider the intermediary as its customer or whether the intermediary should be considered as an introducer and as such be subject to the requirements of section 4.10.

219. Where a relationship has been assessed as being a low risk relationship and where all the requirements of sections 6.5.1 and 6.5.2 are fully met, the financial services business must prepare and retain documentary evidence of the following:

- the adequacy of its process to determine the risk of the business relationship with the intermediary;
- the reasonableness of its conclusions that it is a low risk relationship;
- that it has undertaken CDD procedures in respect of the intermediary – see section 6.5.1; and
- that the relationship relates solely to the provision of financial products or services which meet the requirements of section 6.5.2.

6.5.1 CDD procedures on the intermediary

220. When establishing an intermediary relationship the financial services business in Guernsey must undertake CDD procedures in respect of the intermediary to ensure that the intermediary is:

- an Appendix C business, excluding a trust and corporate service provider, other than a person licensed under the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc. (Bailiwick of Guernsey) Law, 2000 ("Guernsey licensed fiduciary");
- a wholly owned nominee subsidiary vehicle of an Appendix C business, other than a trust and corporate service provider unless it is a Guernsey licensed fiduciary; or
- a wholly owned pension trustee subsidiary vehicle of an Appendix C business, other than a trust and corporate service provider unless it is a Guernsey licensed fiduciary; or
- a firm of lawyers or estate agents operating in Guernsey, and the funds being pooled are to be used for the purchase or sale of Guernsey real estate or leasehold property situated in Guernsey and where the funds received by the firm have been received from a bank operating in Guernsey or a bank from a country or territory listed in Appendix C of the Handbook; and
    - has provided a written confirmation to the financial services

business which:

- confirms that the intermediary has appropriate risk-grading procedures in place to differentiate between the CDD requirements for high and low risk relationships;
- contains adequate assurance that the intermediary conducts appropriate and effective CDD procedures in respect of its customers, including enhanced CDD measures for PEP and other high risk relationships;
- contains sufficient information to enable the financial services business to understand the purpose and intended nature of the business relationship; and
- confirms that the account will only be operated by the intermediary and that the intermediary has ultimate, effective control over the financial product or service.

221. In circumstances where the above criteria are not completely satisfied or are no longer met then the relationship cannot be considered as an intermediary relationship and the financial services business in Guernsey must ensure that appropriate CDD procedures are undertaken in order to comply with the CDD requirements of Regulation 4 and chapter 4.

6.5.2 Products and services

222. For an intermediary to be considered as the customer of the financial services business, a business relationship must be established to provide for one or more of the following products and services:

Product/service	Intermediaries who may be considered as the customer
Investment of life company funds to back the company's policyholder liabilities where the life company opens an account. If the account has a policy identifier then the bank must require an undertaking to be given by the life company that they are the legal and beneficial owner of the funds and that the policyholder has not been led to believe that he has rights over a bank account in Guernsey.	The life company.
The offering of insurance products to another regulated financial services business by a Guernsey licensed insurer, as part of its relationship falling within the scope of the Insurance Law	The regulated financial services business.

Investments via discretionary or advisory investment managers or custodians of their customers' monies into a collective investment scheme either authorised or registered by the Commission where the funds (and any income) may not be returned to a third party unless that third party was the source of funds.	The regulated financial services business, i.e. the discretionary or advisory investment manager or custodian.
Investments via discretionary or advisory investment managers of their customers' monies into a non-Guernsey scheme, where approval has been granted by the Commission to a POI licensee to provide administration, and where the funds (and any income) may not be returned to a third party unless that third party was the source of funds.	The regulated financial services business, i.e. the discretionary or advisory investment manager.
Undertaking various restricted activities by a POI licensee, within the scope of its licence as part of its relationship falling within the scope of the POI Law, with another regulated financial services business licence where the funds (and any income) may not be returned to a third party unless that third party was the source of funds.	The regulated financial services business.
Dealing in bullion by a licensed bank, a POI licensee or a Guernsey licensed fiduciary as part of its relationship with another regulated financial services business, where: • safe custody services are provided in relation to bullion; • no physical bullion is received or delivered; and • any funds may only be received from and/or returned to the intermediary.	The regulated financial services business
The provision of nominee shareholder services	The nominee subsidiary vehicle
The provision of pension trustee	The pension trustee subsidiary vehicle

services to its parent company	
Client accounts held by banks in the name of a POI licensee e.g. a pooled client money account, where the funds are subject to the conduct of business rules.	The POI licensee
Client accounts held by banks in the name of a Guernsey licensed fiduciary 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	The licensed fiduciary or firm of lawyers or estate agents operating in Guernsey.
Pooled accounts held by banks in the name of a Guernsey licensed fiduciary where the holding of funds in the pooled account is on a short-term basis and where the funds (and any income generated) will only be returned to the bank account from which the funds originated. Licensed fiduciaries should ensure that any such use is compatible with relevant trust deeds, and applicable legislation and Codes of Practice.	The Guernsey licensed fiduciary

223. A financial services business should always consider whether it feels the risks would be better managed if the financial services business undertook CDD on the beneficial owner and underlying principal(s) for whom the intermediary is acting rather than treating the intermediary as the customer.

PLEASE NOTE THAT PAGES 67 – 73 HAVE BEEN REPEALED.

THE COMMISSION HAS ISSUED A REVISED WIRE TRANSFERS CHAPTER AS ANNEX II TO THIS HANDBOOK.

CHAPTER 8 – EXISTING CUSTOMERS

Key Regulations

Sections in this Chapter

REGULATIONS

The requirements of the Regulations to which the rules and guidance in this chapter particularly relate are:

- Regulation 3, which provides for a financial services business to identify and assess the risks of money laundering and terrorist financing and to ensure that its policies, procedures and controls are effective and appropriate to the assessed risk. See chapter 3.
- Regulation 4, which provides for the required customer due diligence measures, when they should be applied and to whom they should be applied. See chapter 4.
- Regulation 5, which provides for enhanced customer due diligence measures in respect of business relationships and occasional transactions which have been identified as high risk relationships. See chapter 5.
- Regulation 6, which provides for reduced or simplified customer due diligence measures to be applied to business relationships which have been identified as being low risk relationships. See chapter 6.
- Regulation 8, which makes provisions in relation to anonymous accounts and shell banks. See below.
- Regulation 15, which makes provisions in relation to the review of compliance. See chapter 2.

Regulation 8

8. (1) A financial services business must, in relation to all customers-

(a) not set up anonymous accounts or accounts in fictitious names, and

(b) maintain accounts in a manner which facilitates the meeting of the requirements of these Regulations.

(2) A financial services business must –

(a) not enter into, or continue, a correspondent banking relationship with a shell bank, and

(b) take appropriate measures to ensure that it does not enter into, or continue, a correspondent banking relationship where the respondent bank is known to permit its accounts to be used by a shell bank.

(3) In this regulation -

(a) "**consolidated supervision**" means supervision by a regulatory authority of all aspects of the business of a group of bodies corporate carried on worldwide, to ensure compliance with-

(i) the Financial Action Task Force Recommendations on Money Laundering; and,

(ii) other international requirements,

and in accordance with the Core Principles of Effective Banking Supervision issued by the Basel Committee on Banking Supervision as revised or reissued from time to time,

(b) "**physical presence**" means the presence of persons involved in a meaningful way in the running and management of the bank which, for the avoidance of doubt, is not satisfied by the presence of a local agent or junior staff, and

(c) "**shell bank**" means a bank that has no physical presence in the country or territory in which it is incorporated and licensed and which is not a member of a group of bodies corporate which is subject to effective consolidated supervision.

8 EXISTING CUSTOMERS

A financial services business must comply with the Rules in addition to the Regulations. The Rules are boxed and shaded for ease of reference. A financial services business should note that the Court must take account of the Rules and Guidance issued by the Commission in considering compliance with the Regulations.

8.1 Objectives

264. This chapter provides for the CDD measures to be undertaken in respect of business relationships which have been established with customers taken on before the coming into force of the Regulations.

8.2 Assessing the Risk

265. As identified in chapter 3 a risk-based approach starts with the identification and assessment of the risk that has to be managed. Consideration of the information obtained during the business risk assessment will enable a financial services business to create a profile of a particular business relationship.

266. The adoption of a risk-based approach to the CDD requirements of existing customers allows a financial services business to apply the requirements of this chapter sensibly and to consider all relevant factors rather than carrying out a "tick box" approach.

267. Each financial services business is best placed to assess the risk of its own customer base and the extent and nature of the customer due diligence information held or of any additional documentation or information that may be required for existing customers.

8.3 Customer Due Diligence

268. A financial services business must ensure that its policies, procedures and controls in place in respect of existing customers are appropriate and effective and provide for:

- its customers to be identified;
- the assessment of risk of its customer base;
- the level of CDD to be appropriate to the assessed risk of the business relationship;
- the level of CDD, where the business relationship has been identified as a high risk relationship (for example, a PEP relationship), to be sufficient to allow the risk to be managed;
- the business relationship to be understood; and
- the application of such policies, procedures and controls to be based on materiality and risk.

269. A financial services business should be aware that in accordance with chapters 5 and 6 of the Handbook, enhanced CDD is required for a business relationship which has been identified as a high risk relationship and that where a business relationship has been assessed as being a low risk relationship (for example, locally resident retail customers who have a business relationship which is understood by the financial services business), the information required may be less extensive than that required for new customers.

8.4 Timing

270. In November 2009, the Commission issued Instruction (Number 6) for Financial Services Businesses which required financial services businesses to review the policies, procedures and controls in place in respect of existing customers to ensure that the requirements of regulations 4 and 8 and each of the rules in chapter 8 were met.

271. In order to comply with the requirements of Instruction (Number 6) a financial services business must, by 31 March 2010, have taken any necessary action to remedy any identified deficiencies and satisfy itself that CDD information appropriate to the assessed risk is held in respect of each business relationship.

CHAPTER 9 – MONITORING TRANSACTIONS AND ACTIVITY

Key Regulations

Sections in this Chapter

REGULATIONS

The requirements of the Regulations to which the rules and guidance in this chapter particularly relate are:

- Regulation 11, which provides for the monitoring of transactions and other activity and also for conducting ongoing due diligence. See below.
- Regulation 15, which makes provisions in relation to the review of compliance. See chapter 2.

Regulation 11

11. (1) A financial services business shall perform ongoing and effective monitoring of any existing business relationship, which shall include-

(a) reviewing identification data to ensure it is kept up to date and relevant in particular for high risk relationships or customers in respect of whom there is a high risk,

(b) scrutiny of any transactions or other activity, paying particular attention to all -

(i) complex transactions,

(ii) transactions which are both large and unusual, and

(iii) unusual patterns of transactions,

which have no apparent economic purpose or no apparent lawful purpose, and

(c) ensuring that the way in which identification data is recorded and stored is such as to facilitate the ongoing monitoring of each business relationship.

(2) The extent of any monitoring carried out under this regulation and the frequency at which it is carried out shall be determined on a risk sensitive basis including whether or not the business relationship is a high risk relationship.

9 MONITORING TRANSACTIONS AND ACTIVITY

A financial services business must comply with the Rules in addition to the Regulations. The Rules are boxed and shaded for ease of reference. A financial services business should note that the Court must take account of the Rules and Guidance issued by the Commission in considering compliance with the Regulations.

9.1 Objectives

272. This chapter deals with the requirement for a financial services business to monitor business relationships and to apply scrutiny of unusual, complex or high risk transactions or activity so that money laundering or terrorist financing may be identified and prevented. This may involve requesting additional customer due diligence information.

9.2 Monitoring Business Relationships and Recognising Suspicious Transactions and Activity

273. 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. This may indicate money laundering or terrorist financing activity where the transaction or activity has no apparent economic or visible lawful purpose.

274. Monitoring of the activity of a business relationship must be carried out on the basis of a risk-based approach, with high risk relationships being subjected to an appropriate frequency of scrutiny, which must be greater than may be appropriate for low risk relationships.

275. Transactions and 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.

276. Scrutiny of transactions and activity must be undertaken throughout the course of the business relationship to ensure that the transactions and activity being conducted are consistent with the financial services business' knowledge of the customer, their business, source of funds and source of wealth.

277. A financial services business must consider the possibility for legal persons and legal arrangements to be used as vehicles for money laundering and terrorist financing.

278. A financial services business when monitoring complex, unusual and large transactions or unusual patterns of transactions must examine the background and purpose of such transactions and record such findings in writing.

279. The provision of sufficient and appropriate information and training for staff enables them to recognise potential money laundering and terrorist financing transactions and other activity. Staff screening and training are covered in chapter 11.

280. Reporting of knowledge, suspicion or reasonable grounds for suspicion of money laundering and terrorist financing is addressed in chapter 10.

9.3 Computerised/Manual Monitoring Methods and Procedures

281. Ongoing monitoring of business relationships, including the transactions and other activity carried out as part of that relationship, either through manual procedures or computerised systems, is one of the most important aspects of effective ongoing CDD procedures. A financial services business can usually only determine when it might have reasonable grounds for knowing or suspecting that money laundering or terrorist financing is occurring if they have the means of assessing when a transaction or activity falls outside their expectations for a particular business relationship. The type of monitoring procedures introduced will depend on a number of factors, including the size and nature of the financial services business and the complexity and volume of the transactions or activity.

282. Exception procedures and reports can provide a simple but effective means of monitoring all transactions to or from and activity involving:

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

283. Financial services businesses should tailor the parameters to the nature and level of their transactions and activity and to the assessed risk of the business relationships that are being monitored.

284. A larger or more complex financial services business may also demonstrate ongoing monitoring through the use of computerised systems. Such systems may be used to facilitate the monitoring of significant volumes of transactions or, where the financial services business operates in an e-commerce environment, where the opportunity for human scrutiny of individual transactions and activity is limited.

285. A financial services business should be aware that the use of computerised monitoring systems does not remove the requirement for staff to remain vigilant. It is essential to continue to attach importance to human alertness. Such factors as staff intuition; direct exposure to a customer, face-to-face or on the telephone; and the ability, through practical experience, to recognise transactions and activities that do not seem to have a lawful purpose or make sense for that customer, cannot be automated.

9.4 Ongoing Customer Due Diligence

286. The requirement to conduct ongoing CDD ensures that a financial services business 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 but a financial services business must bear in mind that as the business relationship develops, the risk of money laundering or terrorist financing may change.

287. 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. For example, where there is a material change in the way that the business of the customer is conducted which is inconsistent with its existing business profile.

288. In order to reduce the burden on customers in low risk business relationships, trigger events, for example, the opening of a new account or the purchase of a further product, may present a convenient opportunity to review the CDD information held.

CHAPTER 10 – REPORTING SUSPICION

Key Regulations

Sections in this Chapter

ADDITIONAL LEGISLATION

In addition to the Regulations, rules and guidance in the Handbook there are four other pieces of legislation which have specific requirements with regard to the reporting and disclosure of suspicions.

Financial services businesses must comply with the relevant provisions of the Disclosure (Bailiwick of Guernsey) Law, 2007, the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002, the Disclosure (Bailiwick of Guernsey) Regulations, 2007 and the Terrorism and Crime (Bailiwick of Guernsey) Regulations, 2007. Financial services businesses should note that the Court will take account of the Rules and also of the Guidance provided in the Handbook in considering compliance with the disclosure requirements of this legislation and the Regulations.

The requirements of the legislation to which the rules and guidance in this chapter particularly relate are:

The Disclosure (Bailiwick of Guernsey) Law, 2007

Section 1 and 2 of the Disclosure (Bailiwick of Guernsey) Law, 2007.

http://www.guernseylegalresources.gg/CHttpHandler.ashx?id=71019&p=0

The Disclosure (Bailiwick of Guernsey) Regulations, 2007.

http://www.guernseylegalresources.gg/CHttpHandler.ashx?id=73344&p=0

The Disclosure (Bailiwick of Guernsey) (Amendment) Regulations, 2014.

http://www.guernseyfiu.gov.gg/CHttpHandler.ashx?id=90483&p=0

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

http://www.guernseylegalresources.gg/CHttpHandler.ashx?id=70911&p=0

Sections 15 and 15A of the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002.

The Terrorism and Crime (Bailiwick of Guernsey) Regulations, 2007.

http://www.guernseylegalresources.gg/CHttpHandler.ashx?id=73347&p=0

The Terrorism and Crime (Bailiwick of Guernsey) (Amendment) Regulations, 2014.

http://www.guernseyfiu.gov.gg/CHttpHandler.ashx?id=90482&p=0

REGULATIONS

The requirements of the Regulations to which the rules and guidance in this chapter particularly relate are:

- Regulation 12, which provides for the reporting and disclosing of suspicion. See below.
- Regulation 15, which makes provisions in relation to the review of compliance. See chapter 2.

Regulation 12

12. A financial services business shall –

(a) appoint a person of at least management level as the money laundering reporting officer and provide the name and title of that person to the Commission and the Financial Intelligence Service as soon as is reasonably practicable and, in any event, within fourteen days starting from the date of that person's appointment,

(b) nominate another person to receive disclosures, under Part I of the Disclosure Law and section 15 of the Terrorism Law ("nominated officer"), in the absence of the money laundering reporting officer, and ensure that any relevant employee is aware of the name of that nominated officer,

(c) ensure that where a relevant employee, other than the money laundering reporting officer, is required to make a disclosure under Part I of the Disclosure Law or section 15 of the Terrorism Law, that this is done by way of a report to the money laundering reporting officer, or, in his absence, to a nominated officer,

(d) ensure that the money laundering reporting officer, or in his absence a nominated officer, in determining whether or not he is required to make a disclosure under Part I of the Disclosure Law or section 15A of the Terrorism Law, takes into account all relevant information,

(e) ensure that the money laundering reporting officer, or, in his absence, a nominated officer, is given prompt access to any other information which may be of assistance to him in considering any report, and

(f) ensure that it establishes and maintains such other appropriate and effective procedures and controls as are necessary to ensure compliance with requirements to make disclosures under Part I of the Disclosure Law and sections 15 and 15A of the Terrorism Law.

10 REPORTING SUSPICION

A financial services business must comply with the Rules in addition to the Regulations. The Rules are boxed and shaded for ease of reference. A financial services business should note that the Court must take account of the Rules and Guidance issued by the Commission in considering compliance with the Regulations

10.1 Objectives

289. This chapter outlines the statutory provisions concerning disclosure of information, the policies, procedures and controls necessary for reporting and disclosing suspicion and the provision of information on the reporting and the disclosing of suspicion.

290. References in this chapter to a transaction or activity include an attempted or proposed transaction or activity.

291. References in this chapter to a transaction or activity also include attempted transaction, attempted activity and attempts or proposals to enter into a business relationship or to undertake an occasional transaction.

292. References in this chapter to any suspicion are references to suspicion of either money laundering or terrorist financing.

10.2 Obligation to Report

293. A suspicion may be based upon a 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.

294. It follows that an important precondition of recognition of a suspicious transaction or activity is for the financial services business to know enough about the business relationship and occasional transaction to recognise that a transaction or activity is unusual. Such knowledge would arise mainly from complying with the monitoring and ongoing customer due diligence requirements in Regulation 11 – see chapter 9. Suspicion need not only be based on transactions or activities within the business relationship, but also on information from other sources, including law enforcement agencies, other government bodies, the media, intermediaries, or the customer himself.

295. A financial services business must establish appropriate and effective policies, procedures and controls in order to facilitate compliance with the reporting requirements of the Regulations and the relevant enactments to ensure that:

- each suspicion is reported to the MLRO 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;
- the MLRO promptly considers each such internal suspicion report and determines whether it results in there being knowledge or suspicion or reasonable grounds for knowing or suspecting that someone is engaged in money laundering or terrorist financing;
- where the MLRO has determined that an internal suspicion report does result in there being such knowledge or suspicion or reasonable grounds for so knowing or suspecting that he discloses that suspicion of money laundering or terrorist financing to the FIS – see section 10.4; and
- where, during the CDD process, a financial services business knows or suspects that someone is engaged in money laundering or terrorist financing a disclosure is made to the FIS.

296. The Board of a financial services business 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 a financial services business 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.

297. 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 financial services business would have inferred knowledge or formed the suspicion that another was engaged in money laundering or terrorist financing.

298. 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. For example, an out of the ordinary transaction or activity within a business relationship should prompt the financial services business to conduct enquiries about the transaction or activity – see section 10.6 on tipping off.

299. There may be a number of reasons why the financial services business is not entirely happy with CDD information or where the financial services business otherwise needs to ask questions. Enquiries of their customer should be made where the financial services business has queries, regardless of their level of suspicion, to either assist them in formulating a suspicion, or conversely to negate it, having due regard to the tipping off provisions.

300. Although a financial services business is not expected to conduct the kind of investigation carried out by law enforcement agencies, it must act responsibly and ask questions to satisfy any gaps in the CDD or its understanding of a particular transaction or activity or proposed transaction or activity.

10.3 Internal Reporting

301. A financial services business must have appropriate and effective internal reporting policies, procedures and controls to ensure that:

- all employees of the financial services business know to whom within the financial services business and in what format their suspicions must be reported;
- all suspicion reports are considered by the MLRO and where the MLRO makes a decision not to make a disclosure to the FIS, the reasons for the decision not to disclose are documented and retained; and
- once a disclosure has been made to the FIS, the MLRO immediately informs the FIS where subsequent, relevant information or documentation is received.

302. An example of an internal reporting form is set out in Appendix D1.

10.4 Form and Manner of Disclosing to the FIS

303. Prior to making a disclosure to the FIS the financial services business should consider all available options in respect of the business relationship or occasional transaction.

304. Reports of suspicion of money laundering (including drug money laundering) must be disclosed under the provisions of the Disclosure (Bailiwick of Guernsey) Law, 2007 and suspicions relating to terrorism must be disclosed under the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 as amended. Both of these laws require that information contained in internal reports made to a MLRO is disclosed to the FIS where the MLRO knows or suspects or has reasonable grounds for knowing or suspecting as a result of the report, that a person is engaged in money laundering or terrorist financing.

305. Regulations made under the provisions of the Disclosure Law and of the Terrorism and Crime Law prescribe the manner and form of disclosure. The Disclosure (Bailiwick of Guernsey) (Amendment) Regulations, 2011 and the Terrorism and Crime (Bailiwick of Guernsey) (Amendment) Regulations, 2011 provide that disclosures are to be made through the online reporting facility available on the website of the Financial Investigation Unit at www.guernseyfiu.gov.gg. A copy of the prescribed online form is set out in Appendix D2.

306. The financial services business should provide as much information and documentation (for example, 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.

307. When considering the provision of information to the FIS a financial services business should be aware of the Disclosure (Bailiwick of Guernsey) Law, 2007 and the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002. These laws provide that a disclosure made in good faith to a prescribed 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, both laws provide that disclosures made under them include disclosure of any information or document relating to the knowledge, suspicion or reasonable grounds for suspicion that the person in respect of whom the disclosure is made is engaged in money laundering, and any fact or matter upon which such knowledge, suspicion or reasonable grounds for suspicion is based.

    For the purposes of the above paragraph information or document includes any information or document relating to –

    a) any money or property;
    b) any transaction concerning such money or property; and
    c) the parties to any such transaction.

308. Where the MLRO considers that a disclosure should be made urgently (for example, where the customer's financial services product is already part of a current investigation), initial notification to the FIS may be made by telephone.

309. In addition to the requirements of Regulation 14 for the keeping of records of internal reports a financial services business must also maintain a register of all disclosures made to the FIS pursuant to this paragraph. Such register must contain details of:

- the date of the disclosure;
- the person who made the disclosure;
- the person(s) to whom the disclosure was forwarded; and
- a reference by which supporting evidence is identifiable.

310. To aid communication with the FIS, it may be useful for a financial services business to cross reference its files with the reference number provided by the FIS.

311. The register of disclosures should be reviewed and updated periodically to reflect the current position of each disclosure and of the business relationship. The financial services business should at the time of the review consider whether further communication with the FIS is appropriate.

312. A financial services business must consider whether the nature of the particular suspicion which has been triggered is such that all the assets of the business relationship are potentially suspect. Where it is not possible to separate the assets which are suspicious from the legitimate funds, 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.

313. It is for each financial services business (or group) to consider whether (in addition to any disclosure made in Guernsey) the MLRO should report suspicions within the financial services business (or group), for example, to the compliance department at Head Office. A report to Head Office, the parent or group does not remove the requirement also to disclose suspicions to the FIS.

10.5 The Response of the FIS

314. Disclosures made through the online reporting facility will be immediately acknowledged.

315. If the disclosure does not refer to a specific transaction or activity that could constitute a money laundering or terrorist financing offence, the response from the FIS will simply acknowledge receipt of the disclosure.

316. If the disclosure does include reference to a specific transaction or activity that has led to the suspicion and ultimately a disclosure, the financial services business should indicate whether or not it intends to carry out the transaction or activity, and if so request consent to continue with the particular transaction or activity. The MLRO should exhaust all avenues at his disposal to either negate or confirm whether or not there is a suspicion before seeking consent. On 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, within seven days of receipt of the disclosure, advise in writing its decision regarding the request. In urgent matters, consent may be given orally by the FIS, but will be followed by written confirmation.

317. In the event that consent is not given, the FIS will discuss with the financial services business the implications and will offer what assistance it can in deciding the most appropriate course of action to be taken thereafter. Any such discussion with the FIS does not constitute legal advice. If deemed appropriate, legal advice should be sought by the financial services business from its Advocate or other legal adviser.

318. Access to disclosures will be restricted to appropriate authorities and any information provided by the FIS emanating from such disclosures will normally be in a sanitised format and will not include the identity of the source. In the event of a prosecution, the source of the information will be protected as far as the law allows.

319. The FIS may, by virtue of section 2(1) of the Disclosure (Bailiwick of Guernsey) Regulations, 2007 or section 2(1) of the Terrorism and Crime (Bailiwick of Guernsey) Regulations, 2007, seek additional information from the disclosing financial services business. Such additional information includes financial and administrative information which may provide clarification of the grounds of suspicion and allow the person to whom the disclosure has been made to make a judgement as to how to proceed.

320. 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.

10.6 Communicating with Customers and Tipping Off

321. The Disclosure Law and the Terrorism and Crime Law provide that it is a criminal offence if a person knows, or suspects, that an internal suspicion report to a MLRO or a disclosure to the FIS has been or will be made or if any information or other matter concerning the internal suspicion report or disclosure has been or will be communicated to a MLRO or the FIS and he discloses 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 those laws. Those purposes include, but are not limited to, the prevention, detection, investigation or prosecution of criminal offences, whether in the Bailiwick or elsewhere. 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/CFT responsibilities. A copy of this paper is set out in Appendix E.

322. 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 ongoing monitoring, and should not give rise to tipping off.

323. Policies, procedures and controls must enable a MLRO 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 him with this process. Such procedures must also provide for the MLRO to consider whether it would be more appropriate to decline to proceed with the requested act and to give due thought to the future of the business relationship as a whole.

324. There will be occasions where it is feasible for the financial services business to agree a joint strategy with the FIS, but the FIS will not seek to influence what is ultimately a decision for the financial services business and the online reporting facility cannot be used for this purpose.

10.7 Terminating a Business Relationship

325. Whether or not to terminate a business relationship is a commercial decision except where required by legislation, for example, where the financial services business cannot obtain the required CDD information (see chapter 4 and Regulation 9).

326. Where a financial services business makes a decision to terminate a business relationship after it has made a disclosure or requested consent, and is concerned that, in doing so it may prejudice an investigation or contravene the tipping off rules, it should engage with the FIS accordingly. The decision to terminate a relationship, however, remains with the financial service business.

10.8 Request for Additional Information from Third Parties

The Terrorism and Crime (Bailiwick of Guernsey) (Amendments) Regulations, 2014 and The Disclosure (Bailiwick of Guernsey) (Amendment) Regulations, 2014 inserted a new regulation 2A. The inserted regulation applies where a person has made a disclosure under section 1, 2 or 3 of the Disclosure (Bailiwick of Guernsey) Law, 2007 and/or under the section 12, 15 or 15C of the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 and the police officer to whom the disclosure is made believes as a result, that another person ("a third party") may possess relevant information. A prescribed police officer, 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 may be specified in writing within such period which, in unusual circumstances shall not be less that 7 days, and in such form and manner, as may be specified.

10.9 Definitions

The Terrorism and Crime (Bailiwick of Guernsey) (Amendment) Regulations, 2014 and The Disclosure (Bailiwick of Guernsey) (Amendment) Regulations, 2014 include the following definitions:

- the disclosure upon which the FIS may determine to seek additional information as the 'initial disclosure'.

- the persons from whom additional information is sought as "a third party".

- *The Terrorism and Crime (Bailiwick of Guernsey) (Amendment) Regulations, 2014;* relevant information means information which is, or is likely to be, of assistance to any enquiries that a prescribed police officer reasonably believes to be necessary in order to establish:

    - whether any person is engaged in terrorist financing, or
    - that certain property is or is derived from terrorist property.

- *The Disclosure (Bailiwick of Guernsey) (Amendment) Regulations, 2014;* relevant information means information which is, or is likely to be, of assistance to any enquiries that a prescribed police officer reasonably believes to be necessary in order to establish:

    - whether any person is engaged in money laundering, or
    - that certain property is or is derived from the proceeds of criminal conduct.

10.10 Additional Information Requests

Financial Services Businesses who receive a notice should respond as instructed by the FIS.

PLEASE NOTE THAT PAGES 95 – 113 HAVE BEEN WITHDRAWN

CHAPTER 11 – EMPLOYEE SCREENING AND TRAINING

Key Regulations

Sections in this Chapter

REGULATIONS

The requirements of the Regulations to which the rules and guidance in this chapter particularly relate are:

- Regulation 13, which provides for procedures to be undertaken by a financial services business when hiring employees and for the requirements of training relevant employees. See below.
- Regulation 15, which makes provisions in relation to the review of compliance. See chapter 2.

Regulation 13

13. (1) A financial services business shall maintain appropriate and effective procedures, when hiring employees, for the purpose of ensuring high standards of employee probity and competence.

(2) A financial services business shall ensure that relevant employees receive comprehensive ongoing training in –

(a) the relevant enactments, these Regulations and the Handbook,

(b) the personal obligations of employees and their potential criminal liability under these Regulations and the relevant enactments,

(c) the implications of non-compliance by employees with any rules, Guidance, instructions, notices or other similar instruments made for the purposes of these Regulations, and

(d) its policies, procedures and controls for the purposes of forestalling, preventing and detecting money laundering and terrorist financing.

(3) A financial services business shall identify relevant employees who, in view of their particular responsibilities, should receive additional and ongoing training, appropriate to their roles, in the matters set out in paragraph (2) and must provide such additional training.

11 EMPLOYEE SCREENING AND TRAINING

A financial services business must comply with the Rules in addition to the Regulations. The Rules are boxed and shaded for ease of reference. A financial services business should note that the Court must take account of the Rules and Guidance issued by the Commission in considering compliance with the Regulations.

11.1 Objectives

327. One of the most important tools available to a financial services business to assist in the prevention and detection of money laundering is to have staff who are alert to the potential risks of money laundering and terrorist financing and who are well trained in the requirements concerning CDD and the identification of unusual activity, which may prove to be suspicious.

11.2 Screening of Employees

328. In order for a financial services business to ensure that employees are of the required standard of competence and probity, which will depend on the role of the employee, consideration (which must be documented) must be given to:

- obtaining and confirming appropriate references at the time of recruitment;
- requesting information from the employee with regard to any regulatory action taken against him or action taken by a professional body;
- updates to the lists of specified countries and persons against whom sanctions have been imposed by the United Nations and the European Union on the grounds of suspected or known involvement in terrorist activity;
- requesting information from the employee with regard to any criminal convictions and the provision of a check of his criminal record (subject to the Rehabilitation of Offenders (Bailiwick of Guernsey) Law, 2002); and

must ensure that special attention is paid to and checks undertaken on qualifications and professional memberships relating to potential employees.

329. The term employee as defined in the Regulations includes any person working for a financial services business, i.e. not only individuals working under a contract of employment (including on a temporary basis), but also those working under a contract for services. Where persons who are employees of any third parties carry out work in relation to financial services business under an outsourcing agreement, the financial services business must have procedures to satisfy itself as to the effectiveness of the screening procedures of the third party in ensuring employee competence and probity.

11.3 Relevant Employees

330. The requirements of the Regulations concerning training apply to employees whose duties relate to actual financial services business and any directors or

managers (hereafter referred to as relevant employees), and not necessarily to all employees of a financial services business.

331. When determining whether an employee is a relevant employee, for the purposes of the Handbook a financial services business may take into account the following:

- whether the employee is undertaking any customer facing functions, or handles or is responsible for the handling of business relationships or transactions;
- whether the employee is directly supporting a colleague who carries out any of the above functions;
- 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
- whether an employee's role has changed to involve any of the functions mentioned above.

11.4 Employee Training

332. The Board must be aware of the obligations of the financial services business in relation to staff screening and training.

333. A financial services business must, in ensuring that relevant employees receive the ongoing training required under the Regulations, in particular ensure that they are kept informed of:

- the CDD requirements and the requirements for the internal and external reporting of suspicion;
- the criminal and regulatory sanctions in place for failing to report information in accordance with policies, procedures and controls;
- the identity and responsibilities of the MLRO;
- the principal vulnerabilities of the products and services offered by the financial services business; and
- new developments, including information on current money laundering and terrorist financing techniques, methods, trends and typologies.

334. A financial services business must in providing the training required under the Regulations:

- provide appropriate training to enable relevant employees adequately and responsibly to assess the information that is required for them to judge whether an activity or business relationship is suspicious in the circumstances;
- provide relevant employees with a document outlining their own obligations and potential criminal liability and those of the financial services business under the relevant enactments and the Regulations;
- prepare and provide relevant employees with a copy, in any format, of the financial services business' policies, procedures and controls manual for AML/CFT; and

- ensure its employees are fully aware of legislative requirements.

11.4.1 The MLRO

335. A financial service business is required under the Regulations to identify particular relevant employees who in view of their roles should receive additional training and it must provide such training. Such employees must include, the MLRO, any nominated persons and any deputies to whom suspicion reports may be made. The additional training must include in depth and specific training with regard to;

- the handling and reporting of internal suspicion reports;
- the handling of production and restraining orders including, but not limited to, the requirements of the relevant legislation and how to respond to court orders;
- liaising with law enforcement agencies; and
- the management of the risk of tipping off.

336. Please refer to section 2.4 for information on the role and responsibilities of the MLRO.

11.4.2 The Board and senior management

337. The Board and senior management are responsible for the effectiveness and appropriateness of the financial services business' policies, procedures and controls to counter money laundering and terrorist financing. As such they must be identified as relevant employees to whom additional training must be given in order that they remain competent to give adequate and informed consideration to the evaluation of the effectiveness of those policies, procedures and controls.

338. In addition to the general training provided to relevant employees a detailed level of additional training must be provided to the Board and senior management to provide a clear explanation and understanding of:

- the relevant enactments and the Regulations and information on the offences and the related penalties, including potential director and shareholder liability;
- the CDD and record keeping requirements; and
- the internal and external suspicion reporting procedures.

11.5 Timing and Frequency of Training

339. As part of providing comprehensive ongoing training, appropriate training must be provided for all new relevant employees prior to them becoming actively involved in day-to-day operations. Thereafter, the frequency of training should be determined on a risk-based approach, with those employees with responsibility

for the handling of business relationships or transactions receiving more frequent training.

340. Such programmes may include, as well as the matters required in the Regulations:

- the principal vulnerabilities of any new products, services or delivery channels offered;
- the nature of terrorism funding and terrorist activity, in order that staff are alert to customer transactions or activities that might be terrorist-related;
- information on the changing behaviour and practices amongst money launderers and those financing terrorism;
- emerging typologies; and
- the policies, procedures and controls applied by the financial services business to the assessment of risk and the requirements for dealing with high risk relationships.

341. At a minimum, training must be provided to all relevant employees at least every two years but will need to be more frequent to meet the requirements in the Regulations if new legislation or significant changes to the Handbook are introduced or where there have been significant technological developments within the financial services business.

11.6 The Relevance of Training

342. Whilst there is no single or definitive way to conduct staff training for AML/CFT purposes, the critical requirement is that staff training must be adequate and relevant to those being trained and the training messages should reflect good practice. The training should equip staff in respect of their responsibilities.

343. Financial services businesses must put in place mechanisms to measure the effectiveness of the AML/CFT training.

344. The guiding principle of all AML/CFT 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 financial services business against the risk of money laundering and terrorist financing.

345. The precise approach will depend on the size, nature and complexity of the financial services 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.

346. Training should highlight to employees the importance of the contribution that they can individually make to the prevention and detection of money laundering and terrorist financing. 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 to disseminate

important information because of mistaken assumptions that the information will have already been identified and dealt with by more senior colleagues.

CHAPTER 12 – RECORD KEEPING

Key Regulations

Sections in this Chapter

REGULATIONS

The requirements of the Regulations to which the rules and guidance in this chapter particularly relate are:

- Regulation 14, which provides for the record keeping requirements of a financial services business. See below.
- Regulation 15, which makes provisions in relation to the review of compliance. See chapter 2.

Regulation 14

14. (1) A financial services business shall keep-

(a) a transaction document and any customer due diligence information, or

(b) a copy thereof,

for the minimum retention period.

(2) Where a financial services business is required by any enactment, rule of law or court order to provide a transaction document or any customer due diligence information to any person before the end of the minimum retention period, the financial services business shall-

(a) keep a copy of the transaction document or customer due diligence information until the period has ended or the original is returned, whichever occurs first, and

(b) maintain a register of transaction documents and customer due diligence information so provided.

(3) A financial services business shall also keep records of –

(a) any reports made to a money laundering reporting officer as referred to in regulation 12 and of any disclosure made under Part I of the Disclosure Law or section 15 or 15A of the Terrorism Law made other than by way of a report to the money laundering reporting officer, for five years starting from-

(i) in the case of a report or a disclosure in relation to a business relationship, the date the business relationship ceased, or

(ii) in the case of a report or a disclosure in relation to an occasional transaction, the date that transaction was completed,

(b) any training carried out under regulation 13 for five years starting from the date the training was carried out,

(c) any minutes or other documents prepared pursuant to regulation 15(c) until –

(i) the expiry of a period of five years starting from the date they were finalised, or

(ii) they are superseded by later minutes or other documents prepared under that regulation,

whichever occurs later, and

(d) its policies, procedures and controls which it is required to establish and maintain pursuant to these Regulations, until the expiry of a period of five years starting from the date that they ceased to be operative.

(4) Documents and customer due diligence information, including any copies thereof, kept under this regulation –

(a) may be kept in any manner or form, provided that they are readily retrievable, and

(b) must be made available promptly

(i) to an auditor, and

(ii) to any police officer, the Financial Intelligence Service, the Commission or any other person where such documents or customer due diligence information are requested pursuant to these Regulations or any relevant enactment.

12 RECORD KEEPING

A financial services business must comply with the Rules in addition to the Regulations. The Rules are boxed and shaded for ease of reference. A financial services business should note that the Court must take account of the Rules and Guidance issued by the Commission in considering compliance with the Regulations.

12.1 Objectives

347. Record keeping is an essential component that the Regulations require 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.

12.2 General and Legal Requirements

348. To ensure that the record keeping requirements of the Regulations are met, a financial services business must have appropriate and effective policies, procedures and controls in place to require that records are prepared, kept for the stipulated period and in a readily retrievable form so as to be available on a timely basis, i.e. promptly, to domestic competent authorities upon appropriate authority and to auditors.

12.2.1 Customer due diligence information

349. In order to meet the requirement in the Regulations to keep transaction documents and CDD information a financial services business must keep the following records:

- copies of the identification data obtained to verify the identity of all customers, beneficial owners and underlying principals; and
- copies of any customer files, account files, business correspondence and information relating to the business relationship or occasional transaction; or
- information as to where copies of the CDD information may be obtained.

12.2.2 Transactions

350. In order to meet the requirement 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 financial services business. 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.

351. A financial services business must ensure that in order to meet the record keeping requirements for transactions, documentation is maintained which must include:

- the name and address of the customer, beneficial owner and underlying principal;
- if a monetary transaction, the currency and amount of the transaction;
- account name and number or other information by which it can be identified;
- details of the counterparty, including account details;
- the nature of the transaction; and
- the date of the transaction.

352. Records relating to unusual and complex transactions and high risk transactions must include the financial services business' own reviews of such transactions.

12.2.3 Wire transfer records

353. See section 7.4 of chapter 7 for the record keeping requirements of wire transfer documents.

12.2.4 Internal and external suspicion reports

354. In order to meet the requirement to keep records of reports of suspicion made to a MLRO, a financial services business must keep:

- the internal suspicion report;
- records of actions taken under the internal and external reporting requirements;
- when the MLRO has considered information or other material concerning possible money laundering, but has not made a disclosure of suspicion to the FIS, a record of the other material that was considered and the reason for the decision; and
- copies of any disclosures made to the FIS.

12.2.5 Training

355. Training records must include:

- the dates AML/CFT training was provided;
- the nature of the training; and
- the names of the employees who received training.

12.2.6 Compliance monitoring

356. In order to meet the requirement to keep records of documents prepared in connection with the obligation of the Board to discuss a review of compliance and of its compliance review policy and other policies, procedures and controls relating to compliance, a financial services business must retain:

- reports by the MLRO to the Board and senior management;
- records of consideration of those reports and of any action taken as a consequence; and

- any records made within the financial services business or by other parties in respect of compliance of the financial services business with the Regulations and the Handbook.

12.3 Record Keeping

357. 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 or however they are subsequently retained. A financial services business must, however, consider whether keeping documents other than in original paper form could pose legal evidential difficulties, for example, in civil court proceedings.

12.3.1 Ready retrieval

358. A financial services business must periodically review the ease of retrieval of, and condition of, paper and electronically retrievable records.

359. Where the FIS or another domestic competent authority requires sight of records, under the Regulations or the relevant enactment, which according to a financial services business' procedures would ordinarily have been destroyed, the financial services business must none the less conduct a search for those records and provide as much detail to the FIS or other domestic competent authority as possible.

360. The Regulations require documents which must be kept to be made available promptly to domestic competent authorities where so requested under the Regulations or other relevant enactment. Financial services businesses 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 on introducers or intermediaries.

361. Financial services businesses 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 the Regulations which require records to be readily retrievable.

12.4 Period of Retention

362. The minimum retention periods are set out in Regulation 14.

12.5 Requirements on Closure or Transfer of Business

363. Where a financial services business terminates activities, or disposes of a business or a block of business relationships, for example, by way of asset sale, to another financial service provider the person taking on that business must ensure that the

record keeping requirements in the Regulations are complied with in respect of such business.

CHAPTER 13 – BRIBERY AND CORRUPTION

Applicable Legislation

The Prevention of Corruption (Bailiwick of Guernsey) Law, 2003	Appendix J

Sections in this Chapter

LEGISLATION

In addition to the Regulations, and the Rules and Guidance elsewhere in the Handbook, there is also a dedicated law which has specific requirements with regard to corruption.

The text of the Prevention of Corruption (Bailiwick of Guernsey) Law, 2003 is set out in Appendix J. That text is definitive.

13 BRIBERY AND CORRUPTION

13.1 Objectives

364. Bribery and corruption risk is the risk of a financial services business, or any person acting on behalf of the financial services business, or any third party connected to a business relationship, engaging in bribery or corruption.

365. In light of the increasing global focus on anti-bribery and anti-corruption ("ABC"), the extra-territorial effect of foreign legislation and the links between an effective ABC framework and an effective AML/CFT framework, the Commission is issuing the guidance in this chapter on bribery and corruption. It should be noted that there are currently no rules in this chapter.

366. The objective of this chapter is to provide information about ABC legislation and guidance on how the potential risks of bribery and corruption can be recognised, managed and mitigated. Nothing in this chapter should be read as reducing in any way the requirements of legislation or the rules elsewhere in this handbook.

13.2 Overview

367. The involvement of financial services businesses in corrupt or potentially corrupt practices overseas undermines the integrity of the jurisdiction's financial services sector. Unless robust systems and controls are in place, financial services businesses risk contravening Guernsey and/or overseas ABC legislation. A weak control environment (for example, surrounding the making of payments to overseas third parties) may give rise to the risk of the services of a financial services business being inadvertently used to process potentially corrupt payments.

368. The Board, in the context of its oversight of risk management and maintenance of a sound system of risk identification, measurement and control, has effective responsibility for ensuring that the business complies with the Prevention of Corruption (Bailiwick of Guernsey) Law, 2003 ("the Corruption Law"). The provisions of the Corruption Law apply to corruption committed both within and outside the Bailiwick.

369. The Board also has responsibility for ensuring that the financial services business does not risk contravening the corruption legislation of other jurisdictions which apply to financial services businesses undertaking business in those jurisdictions or which apply to financial services businesses in other ways. For example, the extra-territorial reach of the UK Bribery Act 2010 ("the Bribery Act") means that a foreign company, including a Guernsey company, which carries on any "part of a business" in the UK could be prosecuted under the Bribery Act for failing to prevent bribery committed by any of its employees, agents or other representatives, even if the bribery takes place outside the UK and involves non-UK persons. The Bribery Act also applies to British citizens working anywhere in the world, even if the company for which they work does not carry out business anywhere in the UK.

370. Bribery, corruption and money laundering are criminal acts which are intrinsically linked. By successfully laundering the proceeds of bribery and corruption, the illicit gains may be enjoyed without fear of the proceeds being identified and confiscated.

371. Transparency of transactions and asset ownership is essential to enable the tracing of assets related to corruption and their recovery. Corruption is more likely to flourish in opaque circumstances where the proceeds of such crimes are laundered and cannot be traced back to the underlying corrupt activity, particularly when the ownership and control of assets is obscured, and transactions leave incomplete or misleading audit trails. Effective implementation of the AML/CFT framework increases the transparency of the financial system by creating a reliable trail of information regarding business relationships and the transactions undertaken by them or on their behalf, disclosing the actual ownership control and movement of their assets.

372. The AML/CFT framework requires that financial services businesses pay special attention to any complex, unusual or large transactions, or unusual patterns of transactions that have no apparent or visible economic or lawful purpose. Increased scrutiny is also to be given to high risk customers (such as foreign politically exposed persons ("PEPs")), jurisdictions, high risk business relationships and high risk transactions. These provisions enable the detection of unusual or suspicious activity that might be related to corruption and which must be reported to the FIS.

13.3 Board Responsibility for Oversight of Compliance

373. The Board should have appropriate and effective risk identification and management systems, which include policies, procedures and controls that provide an adequate and effective framework for combating bribery and corruption. In particular, the Board should:

- take responsibility for establishing policies, procedures and controls with regard to ABC;
- take responsibility for the review of compliance with the policies, procedures and controls in place with regard to ABC;
- consider, at regular intervals, the appropriateness and effectiveness of the ABC policies, procedures and controls and take the necessary action to remedy any identified deficiencies; and
- take appropriate measures to keep up to date with, and keep abreast of, bribery and corruption issues.

13.4 Bribery and Corruption Risk Assessment

374. In order to ensure its policies, procedures and controls on ABC are appropriate and effective, a financial services business should assess the potential bribery and corruption risks to which the financial services business could be exposed.

375. It is a matter for each financial services business to consider how it integrates the risk of bribery and corruption into its AML/CFT framework. For example, some

financial services businesses may wish and it may be appropriate to, include the assessment of bribery and corruption risk in their ML/FT business risk assessment.

376. A financial services business should ask itself how it might be exposed to bribery and corruption risk. For example, it should consider what risks are associated with:

- the products/services offered and administered by the financial services business;
- the underlying purpose to which products/services are put e.g. companies set up to invest in high risk industries;
- project financing, particularly where it involves the public sector;
- high value projects or projects involving a significant number of unrelated contractors or third parties;
- the customers of the financial services business and their geographical origin;
- exposure to PEPs;
- the use of and payments to third parties (particularly those located in higher risk jurisdictions)

377. Consideration of the above factors, along with any other factors relevant to the business, will provide a useful framework for the financial services business, having assessed the risk to its business, to tailor its policies, procedures and controls on ABC.

13.5 Relationship Risk Assessment

378. Chapter 3 of this Handbook provides for the undertaking of a relationship risk assessment in respect of any proposed business relationship or occasional transaction. The chapter contains examples of high risk indicators which a financial services business may consider when preparing a risk profile, including indicators associated with bribery and corruption.

13.6 Monitoring Business Relationships

379. As identified in Regulation 11 and chapter 9, an unusual transaction or activity may appear to be inconsistent with the expected pattern of activity within a particular business relationship or the normal business activities for the type of product or service that is being delivered. This may indicate bribery or corruption where the transaction or activity has no apparent economic or visible lawful purpose. Consideration should be given to:

- commission structures, e.g. considering whether commission percentages paid to introducers of new business are reasonable proportionate and transparent;
- charitable or political donations and sponsorship;
- instructions to effect payments for advisory and consulting activities with no apparent connection to the known activities of the business;
- payments to unknown third parties and
- effecting transactions through cash payments and money orders.

13.7 Training

380. As part of the ongoing training of relevant employees, a financial services business should include information about its ABC policies, procedures and controls and the specific risks relating to bribery and corruption to which the business may be exposed.

381. In addition, a financial services business should ensure that those employees responsible for the implementation and monitoring of ABC policies, procedures and controls have additional training in order that they are:

- competent to give adequate and informed consideration to the evaluation of the effectiveness of those policies, procedures and controls; and
- competent to provide adequate and informed input on revisions to those policies, procedures and controls.

13.8 Record Keeping

382. The Board should ensure that appropriate and effective policies, procedures and controls are in place to require that records relevant to ABC are maintained and retained in a readily retrievable form so as to be available on a timely basis, i.e. promptly, to domestic competent authorities upon appropriate authority.

CHAPTER 14 – UN, EU AND OTHER SANCTIONS

Applicable Legislation

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

http://www.guernseylegalresources.gg/article/98999/Terrorist-Asset-Freezing-Bailiwick-of-Guernsey-Law-2011

The Afghanistan (Restrictive Measures) (Guernsey) Ordinance, 2011

http://www.guernseylegalresources.gg/article/93433/Afghanistan-Restrictive-Measures-Guernsey-Ordinance-2011

The Afghanistan (Restrictive Measures) (Alderney) Ordinance, 2011

http://www.guernseylegalresources.gg/CHttpHandler.ashx?id=70430&p=0

The Afghanistan (Restrictive Measures) (Sark) Ordinance, 2011

http://www.guernseylegalresources.gg/CHttpHandler.ashx?id=78298&p=0

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

http://www.guernseylegalresources.gg/article/108694/Al-Qaida-Restrictive-Measures-Guernsey-Ordinance-2013

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

http://www.guernseylegalresources.gg/CHttpHandler.ashx?id=84805&p=0

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

http://www.guernseylegalresources.gg/article/109720/Al-Qaida-Restrictive-Measures-Sark-Ordinance-2013

Sections in this Chapter

LEGISLATION

In addition to the Regulations, and the Rules and Guidance elsewhere in the Handbook, there are also some dedicated enactments which implement sanctions measures relating to terrorist financing and which have specific requirements with regard to making funds or financial services available to listed persons ("the terrorist asset freezing enactments").

The text of the Terrorist Law 2011, the Afghanistan Ordinances and the Al-Qaida Ordinances is accessible by the hyperlinks displayed under applicable legislation.

14. UN, EU AND OTHER SANCTIONS

A financial services business must comply with the Rules in addition to the terrorist asset freezing enactments. In order to assist financial services businesses to understand the contents of the terrorist asset freezing enactments, some of the text below paraphrases the prohibitions which must be observed. Any paraphrasing of that text within this chapter represents the Commission's own explanation of the terrorist asset freezing enactments and is for the purposes of information and assistance only. That paraphrasing does not detract from the legal effect of the terrorist asset freezing enactments or from their enforceability by the courts. In case of doubt you are advised to consult a Guernsey Advocate.

The paraphrased text is contained within a clear box in order to provide clarity whilst the rules which must be followed are boxed and shaded for ease of reference.

14.1 Objectives

383. This chapter outlines the statutory provisions concerning UN, EU and other Sanctions, the policies, procedures and controls necessary in respect of such sanctions and the provision of information on sanctions and freezing of funds notices.

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

384. The Terrorist Law 2011 implements United Nations Security Council Resolution 1373 and Council Regulation (EC) No. 2580/2001 ("the EU Regulation"). The EU regulation imposes restrictive measures directed against certain persons and entities with a view to combating terrorism.

385. The Terrorist Law 2011 prohibits any person from:

(a) dealing with funds or economic resources owned, held or controlled by a designated person, knowing or having reasonable cause to suspect such funds or economic resources are being dealt with;

(b) making funds or financial services available (directly or indirectly) to a designated person knowing or having reasonable cause to suspect, the funds or financial services are being made so available;

(c) making funds or financial services available to any person for the benefit of a designated person, knowing or having reasonable cause to suspect the funds or financial services are being made so available;

(d) making economic resources available (directly or indirectly) to a designated person, knowing or having reasonable cause to suspect that the economic resources are being made so available, and that the designated person would be likely to exchange the economic resources, or use them in exchange, for funds, goods or services;

(e) making economic resources available to any person for the benefit of a designated person, knowing or having reasonable cause to suspect, that the economic resources are being made so available;

(f) intentionally participating in activities, knowing that the object or effect of such activities (whether directly or indirectly) is to circumvent or facilitate the contravention of any of the above prohibitions.

386. A designated person means –

(a) a person designated by Policy Council under the Terrorist Law 2011; or
(b) a person who is the subject of a designation under and within the meaning of the UK's Terrorist Asset-Freezing etc. Act 2010; or
(c) a natural of legal person, group or entity 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 that Regulation is amended from time to time).

387. When determining whether a particular individual or legal person is a designated person, financial services businesses must consult the full list of financial sanctions targets which may be found in the financial sanctions section of the HM Treasury website at: http://www.hm-treasury.gov.uk/fin_sanctions_index.htm

388. The list referred to above is a consolidated list of specified countries, organisations and individuals who have been designated by the United Nations, European Union and United Kingdom under legislation relating to current financial sanctions regimes.

389. Any legal or natural persons designated by the Policy Council who are not on the consolidated lists are named in a separate list maintained by the Policy Council which is accessible on the States of Guernsey website.

390. The disclosure and other requirements of the Terrorist Law 2011 are separate to the requirements of the Disclosure Law and the Terrorism and Crime Law.

14.3 The Afghanistan (Restrictive Measures) (Guernsey) Ordinance 2011 together with corresponding Ordinances for Alderney and Sark ("Afghanistan Ordinances"), and the Al-Qaida (Restrictive Measures) (Guernsey) Ordinance, 2013 and corresponding Ordinances for Alderney and Sark ("Al-Qaida Ordinances").

391. The Afghanistan Ordinances and the Al-Qaida Ordinances implement United Nations Security Council Resolution 1267 ("the original Resolution"). The original Resolution was given effect within the EU by Council Regulation (EC) No. 881/002 ("the original Regulation") which was in turn implemented in the Bailiwick by the Al–Qaida and Taliban (Freezing of Funds) (Guernsey) Ordinance 2011 and corresponding Ordinances for Alderney and Sark. The original Resolution and Regulation, as initially enacted, applied to parties associated with both the Taliban and with Al-Qaida. In 2011, after the death of Osama Bin Laden, the United Nations Security Council created two separate regimes for the Taliban and Al-Qaida. This was done by creating a new regime specific to Afghanistan under United Nations Security Council Resolution 1988, which was based on the list of parties associated with the Taliban that had been listed under the original Resolution. This change was reflected in a corresponding EU Regulation, namely Council Regulation (EU) No. 753/2011 which was then implemented in the Bailiwick by the Afghanistan

Ordinances. The original Regulation continued to apply to parties associated with Al-Qaida and it is currently given effect in the Bailiwick by the Al-Qaida Ordinances.

392. The EU Regulations impose restrictive measures in respect of designated persons, that is, persons, groups or entities designated by the relevant United Nations Sanctions Committees. The lists maintained by those Committees can be accessed at:

http://www.un.org/sc/committees/1988/list.shtml and

http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml.

Persons named in those lists are included in the lists at Annex 1 to each of the two EU Regulations.

393. In order to determine whether any person, group or entity is a designated person, financial services businesses must consult the UN lists as well as the consolidated versions of Annex 1 to each of the two EU Regulations which are accessible at: http://eur-lex.europa.eu/homepage.html

394. The lists in Annex 1 to each of the two EU Regulations are consolidated lists of individuals, groups and entities subject to the sanctions measures and consist of two sections, specified below:

(a) individuals associated with the Taliban or Al-Qaida, as the case may be;

(b) entities and other groups and undertakings associated with the Taliban or Al-Qaida, as the case may be.

395. The Afghanistan Ordinances and the Al-Qaida Ordinances prohibit any person from:

(a) dealing with funds or economic resources belonging to, or owned, held, or controlled by, a designated person;

(b) making available, directly or indirectly, to or for the benefit of a designated person funds or economic resources;

(c) participating knowingly and intentionally in activities with the aim of circumventing the prohibitions, or enabling or facilitating their contravention.

396. The prohibitions in the Afghanistan Ordinances and the Al-Qaida Ordinances are subject to certain exceptions, such as payments due under contracts, agreements or obligations that were concluded or arose before the account became a frozen account, and payment of interest on frozen funds.

397. In addition, the prohibitions do not apply to anything done under the authority of a licence granted by the Policy Council.

14.4 Licences

398. The Policy Council may grant a licence permitting the release of specified funds which would otherwise be caught by the provisions of the Terrorist Law 2011 and of the Afghanistan and Al-Qaida Ordinances. No offence is committed in respect of such funds provided that the terms of the licence are complied with.

399. The Policy Council will entertain applications for licences under the Terrorist Law 2011 and the Afghanistan and Al-Qaida 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.

14.5 Obligation to Report

400. Financial services businesses should note that, under the Terrorist Law 2011 and the Afghanistan and Al-Qaida Ordinances, it is a criminal offence for a financial institution to fail to disclose to the Policy Council its knowledge or suspicion that a customer or potential customer is a designated person or has committed any of the offences set out in the Law or Ordinances. This requirement is additional to the reporting obligation in the Disclosure Law and the Terrorism and Crime Law.

14.6 Obtaining information

401. It should be noted that neither the European Union nor the United Nations has a notification facility for advising when the lists of designated persons maintained by them are updated. However, the consolidated list provided by HM Treasury referred to above includes designations by the European Union and the United Nations and it is kept up to date.

402. The Asset-Freezing Unit of HM Treasury offers a free subscription facility for notification by e-mail when a financial sanctions-related release is published on its website and the consolidated list of targets is updated. Information on how to subscribe for this service is provided on the UN, EU and other sanctions section of the Commission's website, together with the full text of the terrorist asset freezing enactments, information regarding the obligations contained within the enactments and links to both the UN Sanctions Committee lists and the consolidated list of asset freeze targets provided by HM Treasury.

14.7 Information on Guernsey's Sanction Regime

403. In addition to the sanctions regime implemented by the terrorist asset freezing enactments, financial services businesses should be aware that Guernsey has enacted 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.

404. The United Nations and the European Union are key bodies that adopt sanctions measures. Sanctions measures may include:

- financial sanctions including asset freezes and investment bans;
- travel bans;
- import and export bans;
- arms embargos; and
- trade restrictions.

405. Although Guernsey'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.

406. Notwithstanding Guernsey'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 that have extra-territorial effect, so that they may apply to some of the parties involved in a Guernsey transaction on the grounds of nationality or place of incorporation even if the jurisdiction in question is not involved in that transaction.

407. Financial services businesses in Guernsey should be aware, in particular, of sanctions implemented by the US Office of Foreign Assets Controlled (OFAC). OFAC regulations can be applied to:

- U.S. citizens and permanent resident immigrants regardless of where they are located;
- persons and entities within the United States;
- persons and entities trading in U.S. Dollars;
- U.S. incorporated entities and their foreign branches;
- in the cases of certain sanctions, such as those regarding Cuba and North Korea, all foreign subsidiaries owned or controlled by U.S. companies;
- foreign persons in possession of U.S. origin goods in some cases.

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

409. The External Relations Group is mandated on behalf of Policy Council to:

- Agree to implement new sanctions measures;
- License frozen funds; and
- Administer notifications and authorisations (e.g. those under the Iran (Restrictive Measures) (Guernsey) Ordinance, 2010).

410. The Group also works with HM Treasury and the UK's Foreign and Commonwealth Office.

PART 2 – SPECIFIC INDUSTRY SECTORS

CHAPTER 15 – SPECIFIC INDUSTRY SECTORS

Sections in this Chapter

15 SPECIFIC INDUSTRY SECTORS

15.1 Banking

15.1.1 Scope of application

411. Vigilance should govern all the stages of the bank's dealings with its customers, including: account opening; non-account holding customers; safe custody and safe deposit boxes; deposit-taking; lending; transactions into and out of accounts generally, including by way of electronic transfer (wire transfer) and marketing and self-promotion.

412. It needs to be borne in mind that loan and mortgage facilities (including the issuing of credit and charge cards) may be used by launderers at the layering or integration stages. Secured borrowing is an effective method of layering and integration because it puts a legitimate financial business (the lender) with a genuine claim to the security in the way of those seeking to restrain or confiscate the assets.

413. Banks that undertake transactions for persons who are not their account holders should be particularly careful to treat such persons (and any underlying principals) as verification subjects.

414. Particular precautions need to be taken in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such facilities are made available to non-account holders, the verification procedures set out in the Handbook should be followed.

15.1.2 Suspicious features or activities

415. In the absence of a satisfactory explanation the following should be regarded as suspicious activity:

- where a customer is reluctant to provide normal information or provides only minimal, false or misleading information;
- where a customer provides information which is difficult or expensive for the bank to verify;
- opening an account with a significant cash balance and/or subsequent substantial cash deposits, singly or in accumulations without a plausible and legitimate explanation;
- unusual cash deposits without apparent cause, particularly where such deposits are subsequently withdrawn or transferred within a short time;
- frequent small or modest cash deposits which taken together are substantial;
- making use of a third party to deposit cash or negotiable instruments, particularly if these are promptly transferred between client or trust accounts;
- the collection (either within the Bailiwick or in another country or territory) of significant cash sums singly or in accumulations without a plausible and legitimate explanation;

- where a deposit appears to be credited to an account only for the purpose of supporting the customer's order for a bankers' draft, money transfer or other negotiable or readily marketable money or bearer instrument;
- where deposits are received from other banks and the bank is aware of a regular consolidation of funds from such accounts prior to a request for onward transmission of funds;
- the avoidance by the customer or its representatives of direct contact with the bank (such as the use of night safes to make large cash deposits);
- the use of nominee accounts, trustee accounts or client accounts which appear to be unnecessary for or inconsistent with the type of business carried on by the underlying principal;
- the use of numerous accounts for no clear commercial reason where fewer would suffice (so serving to disguise the scale of the total deposits);
- the use by the customer of numerous individuals (particularly persons whose names do not appear on the mandate for the account) to make deposits;
- frequent switches of funds between accounts in different names or in different countries or territories;
- matching of payments out with credits paid in on the same or previous day;
- substantial withdrawal from a previously dormant or inactive account;
- substantial withdrawal from an account which has just received an unexpected large credit from overseas;
- use of bearer instruments outside a recognised dealing system in settlement of an account or otherwise; and
- where a customer declines to provide information which normally would make him eligible for valuable credit or other banking services; or where he inexplicably avoids normal banking facilities, such as higher interest rate facilities for larger credit balances.

15.1.3 Hold mail accounts

416. Hold or retained mail services should only be offered to customers as an exception and should only be provided where plausible and legitimate reasons for requiring the service are given.

15.1.4 Bearer instruments

417. Certain countries or territories permit their companies to issue bearer shares or other instruments as evidence of title. Banks should only open accounts for companies or structures capable of issuing bearer instruments where the holders of the instruments are verified. Banks should take steps to ensure that bearer instruments are held in secure custody by the bank or a trusted intermediary which has undertaken to inform the banks of any proposed change in ownership of the company or structure.

15.2 Fiduciary

15.2.1 Scope of application

418. Fiduciaries should understand the purposes and activities of the structures in relation to which they are appointed or to which they provide services. If they are

unable to do so, they should consider whether a suspicion is raised that assets are, or represent, the proceeds of crime.

15.2.2 Suspicious features or activities

419. If a fiduciary is unable to obtain an adequate explanation of the following features, or any other feature which causes it concern, suspicion could be raised:

- complex networks of trusts and/or nomineeships and/or companies;
- transactions which lack economic purpose (for example, sales or purchases at undervalued or inflated prices; payments or receipts being split between a large number of bank accounts or other financial services products; companies consistently making substantial losses);
- transactions which are inconsistent (for example, in size or source) with the expected objectives of the structure;
- arrangements established with the apparent objective of fiscal evasion;
- structures or transactions set up or operated in an unnecessarily secretive way, for example, involving "blind" trusts, bearer shares, endorsed cheques, cash or other bearer instruments or use of P.O. Boxes;
- lack of clarity about beneficial ownership or interests or difficulties in verifying identity of persons with ownership or control;
- unwillingness to disclose the source of assets to be received by a trust or company;
- unwillingness for the fiduciary to have the degree of information and control which it needs to fulfil its duties;
- use of general powers of attorney in a manner which dilutes the control of a company's directors.

420. When considering whether these or other features cause suspicion, fiduciaries should obtain documentary evidence where appropriate and record explanations they receive.

421. In addition to performing adequate CDD before commencement of the relationship, the fiduciary should, on an ongoing basis, monitor the activities of the structures to which it provides services.

15.3 Investment

15.3.1 Investment Funds

15.3.1.1 Scope of application

422. Investment funds may be open to abuse by people seeking to launder money. The risk of that abuse is increased by the fact that most transactions for subscription, redemption or transfer will not be conducted on a face-to-face basis, and to a similar extent the risk is mitigated by the fact that where some transactions are not conducted on the face-to-face basis, they will typically involve a regulated intermediary or introducer, in Guernsey or elsewhere.

423. To the extent that intermediaries and introducers are regulated in Guernsey, or in a country or territory listed in Appendix C to the Handbook, then financial services businesses may, in the circumstances described in sections 4.10, 4.11 and 6.5 of

the Handbook, rely on the intermediary or introducer to identify the investor and to certify that they have verified the identity of the investor.

424. In order to mitigate the risks of money laundering, firms should take steps to identify any third party subscribers or payees or refuse to accept or make third party payments. Furthermore, most retail investors use these products for medium and long term savings, which makes short-term investment or high turnover unusual and often relatively straightforward to monitor. Where the risks of money laundering are mitigated, then the relevant funds may be considered to be low risk in terms of their use for money laundering purposes. Investors in institutional funds, including private equity funds, may be considered to be of lower risk than their retail counterparts by virtue of the restricted types of investor, rather than the product features. Notwithstanding such consideration it is still necessary to know the identity of such investors.

15.3.1.2 Suspicious features or activities

425. Since most investment is made for medium- and long-term objectives, transactions suggesting that improper use is being made of an investment fund will tend to centre on transactions with very short holding periods (particularly where the investor appears uninterested in mitigating the effect of initial charges).

426. Transactions in open-ended funds, or initial subscriptions at the launch of a closed-ended fund, where funds are to be received from a third party or repaid to a third party, require enhanced due diligence. Funds should not in general be accepted from or paid to a third party without that third party having had its identity verified by the fund operator.

15.3.2 Discretionary and advisory asset management

15.3.2.1 Scope of application

427. In terms of risks associated with money laundering and terrorist financing, there is little distinction between discretionary and advisory asset management activities. In both cases the customer will usually need to have been subject to full assessment at take on, both in order to verify identity and source of funds, and it will in any case be necessary to review the customer's objectives in order to assess, for other regulatory reasons, the suitability of transactions undertaken or recommended for the customer.

15.3.2.2 Suspicious features or activities

428. Consideration should be given to undertaking enhanced due diligence where there are frequent and unexplained additions to the investment portfolio, and or where there are frequent and unexplained requests for assets to be realised and the funds paid away. As with investment funds, receipt of funds from, or remission of funds to, third parties should not be undertaken unless there is a satisfactory explanation for the arrangement and the identity of the third party has been verified by the service provider.

15.3.3 Intermediaries

429. The paragraphs below should be read together with section 6.5 of the Handbook.

15.3.3.1 Scope of application

430. Intermediaries may provide stock broking services and also act as interface between the investor and other investment product providers. As with discretionary and advisory asset managers, intermediaries will need to have set up, under Guernsey regulatory rules, a full customer agreement with any potential customer and will need to assure themselves the suitability of any recommendation they make. They will therefore need to have researched and verified the customer's identity, source of funds and investment objectives in order to provide that service in accordance with the requirements of the Regulations and the Handbook.

431. "Execution Only" arrangements, in which the service provider is not required to assess the suitability of any transaction for the customer, can be a feature of intermediary business. That would not absolve the intermediary from a knowledge and verification of a customer's identity and source of funds.

15.3.3.2 Suspicious features or activities

432. As with investment fund operators, and discretionary and advisory asset managers, intermediaries will need to be vigilant as to the source and use of the assets which they are invited to trade. In particular, intermediaries will need to make enquiries in circumstances where there are sudden and unexplained additions to, or transfers from, the client's investment portfolio.

433. Intermediaries will also be on enquiry in circumstances where the client appears indifferent to the profit or loss generated by trading activities.

434. Intermediaries will also need to make enquiries where the client transfers, and asks the intermediary to dispose of, assets which were not acquired through that intermediary, since transfers of assets off market may provide a vehicle for the laundering of money.

15.4 Insurance

15.4.1 Scope of application

435. Insurers, insurance managers, and the introducers of insurance business are responsible for transactions which present a number of opportunities for money laundering and the financing of terrorism. As such the proper identification of the sources of funding for these transactions, the purposes of these transactions and the ultimate benefit of these transactions should be fully understood and documented by licensees. If an insurance licensee is faced with a transaction which it cannot fully explain and document, then suspicion should be raised if subsequent enquiries do not provide plausible explanation.

15.4.2 Suspicious features or activities

436. In the absence of a satisfactory explanation the following should be regarded as suspicious activity:

- the purchase of a significant single premium product followed by the early surrender or termination of the policy where this gives rise to a loss, or to a payment to an unusual third party;
- the use of trusts within the ownership structure of a managed insurer;
- transactions which are inconsistent in size or source with the expected business plan and cash-flow projections of the licensee;
- transactions which are either priced at a level which is significantly out of line with current market rates, or where claims incidence is significantly out of line with current market loss ratios;
- introductions from brokers or agents based in countries or territories with which the licensee is unfamiliar, or from which criminal or terrorist funding activity is known or suspected to occur;
- overly complex or confusing transactions, including any transactions involving a number of counterparties or multi-jurisdictional entities;
- insurance transactions giving rise to unusually large or uneconomic commission payments or expenses, especially where the payments are to unrelated or unknown recipients;
- bearer shares within the ownership structure of a licensee, or bearer instruments used to fund the premiums or capital of a licensee;

- individuals or corporate entities based in unregulated or loosely regulated countries or territories, especially where there are difficulties or undue delays in obtaining information in respect such individuals or entities;
- receipts or payments which appear to have little or no economic value, or where such receipts or payments are split between a large number of counterparties;
- introductions from clients in overseas countries or territories where comparable policies are available "closer to home";
- transactions involving cash payments from unusual third parties, or where settlement directions are for the benefit of unusual third parties rather than the policyholder;
- early termination of policies, especially at a loss, and/or when the repayment request is for the benefit of a third party, or in a different form to the initial premium payment.

437. Illustrations of the type of situation that might give rise to reasonable grounds for suspicion in some circumstances are:

- transactions or instructions which have no apparent purpose and which make no obvious economic sense;
- where the transaction being requested by the customer, without reasonable explanation, is out of the ordinary range of services normally provided or is outside the experience of the financial services business in relation to the particular customer, customer profile or business relationship;
- transfers to and from high risk countries or territories without reasonable explanation;
- where the customer refuses to provide routine information requested by the financial services business without reasonable explanation;
- where a customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period of time;

- unusual patterns of payment such as unnecessary routing of funds through third party accounts, cash payments (receipts or collection), making more than one payment or making payments to a variety of accounts where one would normally be expected; and
- requests for hold mail facilities without legitimate purpose.

15.5 General

15.5.1 Suspicious features or activities

438. In the absence of a satisfactory explanation the following might give grounds for suspicion in some circumstances:

- unusual early cancellation of any financial products or services that result in an economic penalty to the customer;
- large numbers of individuals making payments into one account;
- customers who have accounts with many financial services businesses in the same jurisdiction;
- frequent requests for travellers cheques, drafts or other negotiable instruments or frequent paying of funds using these types of instruments;
- frequent and seemingly unnecessary currency exchanges;
- unexpected repayment activity on loans;
- the use of a financial product as a loan collateral in unusual circumstances (for example, the purchase of a product which is immediately used as collateral);
- transactions that are at economically disadvantageous terms for the customer;
- transactions with last minute amendments to settlement instructions or changes to a third party settlement;
- advice being requested on a capital structure or industrial strategy where the arrangement is not characteristic of the customer's profile.

PART 3 – APPENDICES AND GLOSSARY

CHAPTER 16 – APPENDICES

Appendices in this Chapter

16 APPENDICES

APPENDIX A

GENERAL INTRODUCER CERTIFICATE GIC1

Name of accepting financial services business		
Name of Introducer		
Account name (in full)		
Details of associated account/s (which are part of the same structure)		
Introducer's contact details	**Address:**	
	Telephone:	**Fax:**
	Email:	

The Introducer certifies that it is a Guernsey licensed financial services business or an Appendix C business and in respect of this account it has obtained and holds the verification required to satisfy the Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing ("Handbook") issued by the Guernsey Financial Services Commission, as updated from time to time. The information disclosed for this account by the Introducer accurately reflects the information held and is being given for account opening and maintenance purposes only. The Introducer undertakes to supply certified copies or originals of the verification documentation upon request without delay.

Signature: _____ _____

Full Name: _____ _____

Official Position: _____ _____

Date: _____ _____

Please identify the number of supplementary pages being submitted: GIC2 ☐ GIC3 ☐ GIC4 ☐

APPENDIX A (CONTINUED)

GENERAL INTRODUCER CERTIFICATE GIC2
IDENTIFICATION INFORMATION

Name of Introducer: _____

Account name (in full): _____

To be completed for applicants for business who are individuals or partners in a partnership only
(Please complete the section below and attach additional copies of this sheet as required)

	1	2
Full Name		
Nationality, date and place of birth		
Current residential address (please include postcode). Note: A PO Box only address is insufficient		
Does the Introducer consider the related party to be, or to be associated with a PEP?	Yes ☐ No ☐	Yes ☐ No ☐

To be completed for applicants for business who are companies, partnerships, trusts or foundations

Date of incorporation or registration (if applicable)		Registration number	
Place of incorporation or registration (if applicable)			
Current registered office address (if applicable)			
Date of establishment (if unincorporated/unregistered)		legal jurisdiction (if unincorporated /unregistered)	
Type of trust/foundation/company			
Is it a trading entity Yes ☐ No ☐	Are bearer shares currently in issue? Yes ☐ No ☐	If no, can bearer shares be issued? Yes ☐ No ☐	

To be completed for all applicants for business

Nature of activities or purpose and intended nature of business relationship (please provide full description)	
(for all PEP relationships and, where appropriate, for high risk relationships): Source of wealth (and identify the period over which this has been derived)	
Account activity	

Should the space provided be insufficient, please continue using GIC4.

Initial of signatory /ies completing GIC1		

APPENDIX A (CONTINUED)

GENERAL INTRODUCER CERTIFICATE GIC3
RELATED PARTIES

Name of Introducer: _____

Account name (in full): _____

Details of all principal(s) (see GIC5 for definition) including beneficial owners and excluding officers of the Introducer

(Please complete the section below and attach additional copies of this sheet as required)

	1	2
Full Name		
Nationality, date and place of birth		
Current residential address (please include postcode). Note: A PO Box only address is insufficient		
Role of principal and date relationship commenced		
Does the Introducer consider the related party to be, or to be associated with a PEP?	Yes ☐ No ☐	Yes ☐ No ☐

	3	4
Full Name		
Nationality, date and place of birth		
Current residential address (please include postcode). Note: A PO Box only address is insufficient		
Role of principal and date relationship commenced		
Does the Introducer consider the related party to be, or to be associated with a PEP?	Yes ☐ No ☐	Yes ☐ No ☐

Initial of signatory /ies completing GIC1		

APPENDIX A (CONTINUED)

GENERAL INTRODUCER CERTIFICATE GIC4
ADDITIONAL INFORMATION

Name of Introducer: _____

Account name (in full): _____

This section is to be used by the financial services business to identify any additional information or documentation that they require over and above the stated minimum and/or for the Introducer to provide additional information to supplement the details contained in GIC1, GIC2 and/or GIC3.

Initial of signatory /ies completing GIC1		

APPENDIX A (CONTINUED)

GENERAL INTRODUCER CERTIFICATE GIC5
NOTES AND GUIDANCE

These notes and the definitions below are intended to assist the Introducer in completing the required forms and to enable greater consistency to be achieved.

"Associated accounts"	Refers to an account with the same financial services business where any of the principals are connected with an account in the same group or structure.
"Account activity"	An estimate of the total flow of funds in and out of the account should be provided. An estimated maximum account turnover should also be provided. For a trading operation, the scale and volume of transactions should be explained.
"Bearer shares"	Should bearer shares be subsequently issued (after the opening of the account) such that the "Yes" box needs ticking in GIC2, an updated form should be supplied to the accepting financial services business without delay.
"Certified copy"	An officer or authorised signatory of a regulated financial services business will be an acceptable certifier. An acceptable "certified copy" document should be an accurate and complete copy of the original such that the certifier will sign and date the copy document printing his position, capacity and company name.
"Introducer"	Is a Guernsey licensed financial services business or an Appendix C business.
"Nature of activities or purpose and intended nature of business relationship"	A sufficient description should be provided to enable the accepting financial services business to properly categorise the underlying nature of the arrangements. If the activity is of commercial nature, then additional information may be required.
"PEP"	Politically exposed person as defined in the Handbook.
"Principal"	Includes any person or other entity that has or is likely to receive a benefit in the foreseeable future or who the Introducer customarily treats as having an economic interest.
"Role"	This might include, for example, a beneficial owner, a shareholder, beneficiary, settlor, partner, etc.
"Signatory"	The Introducer's Certificate will need to be signed or initialled (where appropriate) in line with the Introducer's current mandate/authorised signatory list held with the accepting financial services business.
"Source of wealth"	The origins of the wealth of the principal/s (and over what period) should be identified. Generally, simple one word answers will be unacceptable, for example, "income", "dividends", "Bill Smith", or "work". A brief description to give a fuller picture is expected, for example, "sale of UK private company in 1997", "life time savings of settler who was a doctor", "inheritance from parents' UK estate" and "UK property development over the last 10 years".
"Trading"	Implies commercial activity which may include a business, invoicing or re-invoicing operations. For clarity, a "trading company" does not include a personal service/employment company.

Please refer to the accepting financial services business should you have any doubt or queries about completing the Introducer Certificate Forms.

APPENDIX B

GUERNSEY FIDUCIARY INTRODUCER CERTIFICATE FIC1

Name of bank/deposit taker or accepting financial services business		
Name of Introducer		
Account name (in full)		
Details of associated account/s (which are part of the same structure)		
Introducer's contact details	**Address:**	
	Telephone:	**Fax:**
	Email:	

The Introducer certifies that it is a Guernsey licensed financial services business and in respect of this account it has obtained and holds the verification required to satisfy the Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing ("Handbook") issued by the Guernsey Financial Services Commission, as updated from time to time. The information disclosed for this account by the Introducer accurately reflects the information held and is being given for account opening and maintenance purposes only. The Introducer undertakes to supply certified copies or originals of the verification documentation upon request without delay.

Signature: _____ _____

Full Name: _____ _____

Official Position: _____ _____

Date: _____ _____

Please identify the number of supplementary pages being submitted: FIC2 ☐ FIC3 ☐ FIC4 ☐

APPENDIX B (CONTINUED)

GUERNSEY FIDUCIARY INTRODUCER CERTIFICATE FIC2
IDENTIFICATION INFORMATION

Name of Introducer: _____

Account name (in full): _____

To be completed for applicants for business who are companies, partnerships, trusts or foundations

Date of incorporation or registration (if applicable)		Registration number	
Place of incorporation or registration (if applicable)			
Current registered office address (if applicable)			
Date of establishment (if unincorporated/unregistered)		legal jurisdiction (if unincorporated /unregistered)	
Type of trust/foundation/company			

Is it a trading entity Yes ☐ No ☐	Are bearer shares currently in issue? Yes ☐ No ☐	If no, can bearer shares be issued? Yes ☐ No ☐

To be completed for all applicants for business

Nature of activities or purpose and intended nature of business relationship (please provide full description):	
(for all PEP relationships and, where appropriate, for high risk relationships): Source of wealth (and identify the period over which this has been derived)	
Account activity	

Should the space provided be insufficient, please continue using FIC4.

Initial of signatory /ies completing FIC1		

APPENDIX B (CONTINUED)

GUERNSEY FIDUCIARY INTRODUCER CERTIFICATE FIC3
RELATED PARTIES

Name of Introducer: _____

Account name (in full): _____

Details of all principal(s) (see FIC5 for definition) including beneficial owners and excluding officers of the Introducer

(Please complete the section below and attach additional copies of this sheet as required)

	1	2
Full Name		
Nationality, date and place of birth		
Current residential address (please include postcode). Note: A PO Box only address is insufficient		
Role of principal and date relationship commenced		
Does the Introducer consider the related party to be, or to be associated with a PEP?	Yes ☐ No ☐	Yes ☐ No ☐

	3	4
Full Name		
Nationality, date and place of birth		
Current residential address (please include postcode). Note: A PO Box only address is insufficient		
Role of principal and date relationship commenced		
Does the Introducer consider the related party to be, or to be associated with a PEP?	Yes ☐ No ☐	Yes ☐ No ☐

Initial of signatory /ies completing FIC1		

APPENDIX B (CONTINUED)

GUERNSEY FIDUCIARY INTRODUCER CERTIFICATE FIC4
ADDITIONAL INFORMATION

Name of Introducer: _____

Account name (in full): _____

This section is to be used by the bank/deposit taker to identify any additional information or documentation that they require over and above the stated minimum and/or for the Introducer to provide additional information to supplement the details contained in FIC1, FIC2 and/or FIC3.

Initial of signatory /ies completing FIC1		

APPENDIX B (CONTINUED)

GUERNSEY FIDUCIARY INTRODUCER CERTIFICATE FIC5 NOTES AND GUIDANCE

These notes and the definitions below are intended to assist the Introducer in completing the required forms and to enable greater consistency to be achieved.

"Associated accounts"	Refers to an account with the same financial services business where any of the principals are connected with an account in the same group or structure.
"Account activity"	An estimate of the total flow of funds in and out of the account should be provided. An estimated maximum account turnover should also be provided. For a trading operation, the scale and volume of transactions should be explained.
"Bearer shares"	Should bearer shares be subsequently issued (after the opening of the account) such that the "Yes" box needs ticking in FIC2, an updated form should be supplied to the accepting financial services business without delay.
"Certified copy"	An officer or authorised signatory of a regulated financial services business will be an acceptable certifier. An acceptable "certified copy" document should be an accurate and complete copy of the original such that the certifier will sign and date the copy document printing his position, capacity and company name.
"Introducer"	Is a local regulated financial services business as defined in the Handbook.
"Nature of activities or purpose and intended nature of business relationship"	A sufficient description should be provided to enable the accepting financial services business to properly categorise the underlying nature of the arrangements. If the activity is of commercial nature, then additional information may be required.
"PEP"	Politically exposed person as defined in the Handbook.
"Principal"	Includes any person or other entity that has or is likely to receive a benefit in the foreseeable future or who the Introducer customarily treats as having an economic interest.
"Role"	This might include, for example, a beneficial owner, a shareholder, beneficiary, settlor, partner, etc.
"Signatory"	The Introducer's Certificate will need to be signed or initialled (where appropriate) in line with the Introducer's current mandate/authorised signatory list held with the accepting financial services business.
"Source of wealth"	The origins of the wealth of the principal/s (and over what period) should be identified. Generally, simple one word answers will be unacceptable, for example, "income", "dividends", "Bill Smith", or "work". A brief description to give a fuller picture is expected, for example, "sale of UK private company in 1997", "life time savings of settler who was a doctor", "inheritance from parents' UK estate" and "UK property development over the last 10 years".
"Trading"	Implies commercial activity which may include a business, invoicing or re-invoicing operations. For clarity, a "trading company" does not include a personal service/employment company.

Please refer to the accepting financial services business should you have any doubt or queries about completing the Introducer

APPENDIX C

COUNTRIES OR TERRITORIES WHOSE REGULATED FINANCIAL SERVICES BUSINESSES MAY BE TREATED AS IF THEY WERE LOCAL FINANCIAL SERVICES BUSINESSES

Australia
Austria
Belgium
Bermuda
Bulgaria
Canada
Cayman Islands
Cyprus
Denmark
Estonia
Finland
France
Germany
Gibraltar
Greece
Hong Kong
Hungary
Iceland
Ireland
Isle of Man
Italy
Japan
Jersey
Latvia
Liechtenstein
Lithuania
Luxembourg
Malta
Netherlands
New Zealand
Norway
Portugal
Singapore
Slovenia
South Africa
Spain
Sweden
Switzerland
United Kingdom
United States of America

Appendix C to the Handbook was established to reflect those countries or territories which the Commission considers require regulated financial services businesses to have in place standards to combat money laundering and terrorist financing consistent with the FATF Recommendations and where such financial services businesses are supervised for compliance with those requirements. It was also designed as a mechanism to recognise the geographic spread of the customers of the Guernsey 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 money laundering and terrorist financing that are consistent with the FATF Recommendations means only that the necessary legislation and other means of ensuring compliance with the Recommendations is in force in that country or territory. It does not provide assurance that a particular overseas financial services business is subject to that legislation, or that it has implemented the necessary measures to ensure compliance with that legislation.

Guernsey financial services businesses are not obliged to deal with regulated financial services businesses in the jurisdictions listed above as if they were local, notwithstanding that they meet the requirements identified in this Appendix. Guernsey financial services businesses should use their commercial judgement in considering whether or not to deal with a regulated financial services business and may, if they wish, impose higher standards than the minimum standards identified in the Handbook.

In accordance with the definition provided for in the Regulations an "A**ppendix 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 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 on Money Laundering 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.

The absence of a country or territory from the above list does not prevent the application of section 4.10.1 of the Handbook (reliable introductions by an overseas branch or member of the same group, subject to satisfactory terms of business).

APPENDIX D1

INTERNAL REPORT FORM

Name of Customer			
Full account name(s)			
Account/product number(s)			
Date(s) of opening			
Date of customer's birth			
Nationality			
Passport number			
Identification and reference			
Customer's address			
Details arousing suspicion			
As relevant:	Amount (currency)	Date of receipt	Source of funds
Other relevant information			
Money Laundering Reporting Officer *			
Name of Employee			
Date of Report			

** The Money Laundering Reporting Officer should briefly set out the reason for regarding the transactions to be reported as suspicious, or if he decides against reporting, the reasons for that decision.*

APPENDIX D2

DISCLOSURE FORM
STRICTLY PRIVATE AND CONFIDENTIAL

Please forward with covering letter to: The Guernsey Border Agency, Financial Investigation Unit: Financial Intelligence Service, Ozanne Hall, Mignot Plateau, Cornet Street, St Peter Port, GY1 1LF Tel: 714081 Fax: 710466 E-mail: fiu@gba.gov.gg	
Reporting MLRO:	
Tel:	Email:

Your reference		
FIS reference		
Date		Consent request? **Yes/No**

1. MAIN DISCLOSURE SUBJECT

Person

Title	
Full name *(please include former and other names)*	
Is the subject a Politically Exposed Person? *(please give details)*	
Gender	
Date of birth /Alias date of Birth	
Estimated age	
Place of Birth	
Town of Birth	
Nationality(ies)	
Occupation	

APPENDIX D2 (CONTINUED)

Employer	
Address(es) including postal codes	
Country of Residence	
Contact details, e.g. telephone, fax, email	
Passport number(s) and dates	
Passport issuing country(ies)	
Other identification numbers and dates, e.g. national identity card, driving licence etc. *(please specify type)*	
Any other relevant information	

and/or Organisation

Type of Organisation i.e. company, trust, non-profit organisation or other	
Name *(please include former and other names)*	
Legal registration / identification number	
Address(es) including postal codes	
Contact details, e.g. telephone, fax, email	
Place of incorporation / date	
Country registered / established	
Date registered / established	
Any other relevant information	
(*Trust*) Country of Administration Country Settled	
(*non-profit organisation*) Area of Benefit Area of Operation	

APPENDIX D2 (CONTINUED)

2. ASSOCIATED SUBJECTS (including organisation officials)

Official Type	
Title	
Full name *(please include former and other names*	
Date of birth	
Address(es) including postal codes	

For further associated subjects, please copy the formats used above

3. RELEVANT ACCOUNTS

Account Name	
Account Holder(s)	
Financial Institution/ SWIFT/BIC address	
Account / product type, e.g. investment, company etc.	
Account number and sort code	
Date account opened	
Date account closed	
Account balance / value	
Balance / value date	

For additional accounts or products, please copy the format used above.

4. RELEVANT TRANSACTIONS

Please note that the obligation to report suspicion applies to all types of transaction and attempted transaction, including attempted transactions in circumstances where there is no existing business relationship with the disclosure subject and no such business relationship is subsequently established.

Transaction date	
Transaction amount	
Transaction type / method	
Transaction parties *(please use person / organisation format as above where more detailed information is available)*	
Was the transaction carried out?	

APPENDIX D2 (CONTINUED)

Was the transaction made in the context of an existing business relationship? If not, was a business relationship then established?	

For additional transactions, please copy the format used above.

5. CLIENT RELATIONSHIP

Current status of relationship	
Date relationship commenced	
Date relationship ended	

6. REASONS FOR SUSPICION

Please give full account of circumstances and grounds for suspicion

Suspected Underlying Offences	*Please specify where possible the nature of the offences which you suspect may underlie or otherwise be relevant to the transaction, for example fraud or corruption, (whether carried out or not), together with the grounds for that suspicion.*

This disclosure is made under the *(please delete as appropriate)*	Terrorism and Crime (Bailiwick of Guernsey) Law, 2002
	Disclosure (Bailiwick of Guernsey) Law, 2007

7. DETAILS OF ANY REQUEST FOR CONSENT

Please specify the act or transaction for which consent is sought

8. ADDITIONAL INFORMATION (including explanation of any attachments)

NB - Please also provide as much information and documentation 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, e.g. copy identification and account opening documents, account statements, contract notes, minutes, correspondence, structure charts, transcripts, etc.

APPENDIX D3

SPECIMEN CONSENT NOT REQUIRED OF THE FIS

MLRO

Your Ref :
FIS Ref :

PRIVATE & CONFIDENTIAL - ADDRESSEE ONLY

Dear

Thank you for the disclosure of information you have provided under the provisions of the Disclosure (Bailiwick of Guernsey) Law, 2007 concerning:-

XXXXXXXXX

Your suspicions have been noted.

Based upon the information provided please note that this is not a consent issue.

This does not release you from your obligation in respect of all future transactions on the account or arising from the relationship to comply with the relevant anti money laundering legislation and to have due regard to the Guernsey Financial Services Commission Handbook on countering financial crime and terrorist financing.

Thank-you for your continued co-operation.

Yours sincerely

APPENDIX D4

SPECIMEN CONSENT OF THE FIS

MLRO

Your Ref :
FIS Ref :

PRIVATE & CONFIDENTIAL - ADDRESSEE ONLY

Dear

Thank you for the disclosure of information you have provided under the provisions of the Disclosure (Bailiwick of Guernsey) Law, 2007 concerning *[insert subject here]*

Your suspicions have been noted.

Based upon the information provided you have consent to continue or maintain the account(s) or other relationship.

This does not release you from your obligation in respect of all future transactions on the account or arising from the relationship to comply with the relevant anti money laundering legislation and to have due regard to the Guernsey Financial Services Commission Handbook on countering financial crime and terrorist financing.

Thank you for your continued co-operation.

Yours sincerely

APPENDIX D5

SPECIMEN CONSENT REFUSED OF THE FIS

MLRO

Your Ref :
FIS Ref :

PRIVATE & CONFIDENTIAL - ADDRESSEE ONLY

Dear

Thank you for the disclosure of information you have provided under the provisions of the Disclosure (Bailiwick of Guernsey) Law, 2007 concerning: -

XXXXXXXXX

Your suspicions have been noted.

Based upon the information provided you do not have consent to: XXXXXXXXX

This does not release you from your obligation in respect of all future transactions on the account or arising from the relationship to comply with the relevant anti money laundering legislation and to have due regard to the Guernsey Financial Services Commission Handbook on countering financial crime and terrorist financing.

Thank-you for your continued co-operation.

Yours sincerely

APPENDIX D6

SPECIMEN ACKNOWLEDGMENT OF THE FIS

MLRO

Your Ref :
FIS Ref :

PRIVATE & CONFIDENTIAL - ADDRESSEE ONLY

Dear

Thank you for the disclosure of information you have provided concerning:

XXXXXXXXXX

The information has been noted.

Thank you for your continued co-operation.

Yours sincerely

APPENDIX E

GUIDANCE ON PROSECUTION FOR TIPPING OFF

This guidance is issued by HM Procureur in his capacity as the prosecuting authority within the Bailiwick and it does not constitute legal advice. Anyone who has concerns about any of the matters covered in this guidance should obtain independent legal advice. A glossary of terms used in this document is set out at the end.

BACKGROUND

It has come to the attention of the Bailiwick authorities that the finance industry and others would welcome clarification of the reach of the tipping off offences. Amendments to the Disclosure Law and the Terrorism Law are under consideration. In the meantime, this guidance is issued to clarify the circumstances in which prosecution will be pursued. It may be revoked or amended at any time.

THE TIPPING OFF OFFENCES

The tipping off offences were introduced to underpin the regime for making SARS (that is, required disclosures) under the Disclosure Law and the Terrorism Law. Their purpose is to prevent the subject of a SAR or other person from causing prejudice to ongoing or future investigations into money laundering or terrorist financing as the case may be. In order to achieve this, it is important that as few people as possible are aware that a SAR has been made. For this reason the scope of the offences is necessarily very wide, with a correspondingly narrow range of exemptions, and the offences carry substantial penalties.

However, it was not and is not the intention of the Bailiwick authorities that the tipping off offences should forestall legitimate attempts to prevent money laundering and terrorist financing. It is extremely important that those working in the finance sector and other affected industries are content that they are able to communicate concerns if they are to discharge their AML/CFT responsibilities effectively.

PROSECUTION

For the avoidance of doubt it is confirmed that no prosecutions will be brought against persons who disclose the fact that a SAR has been or will be made, if the disclosure is made by one member of an organisation to another for the purposes of discharging AML/CFT responsibilities and functions. This will also be the case in respect of a disclosure made to linked organisations such as head offices or other branches of the same institution, again providing that it is made to discharge AML/CFT responsibilities and functions.

However, this will not apply if the disclosure is made in circumstances where there are grounds to believe that it may prejudice an investigation.

HM Procureur
October 2011

GLOSSARY

AML/CFT	Anti –Money Laundering/Countering the Financing of Terrorism
Disclosure Law	Disclosure (Bailiwick of Guernsey) Law 2007
MLRO	Money Laundering Reporting Officer
SAR	Suspicious Activity Report
Terrorism Law	Terrorism and Crime (Bailiwick of Guernsey) Law 2002
Tipping Off Offences	Offences at section 4 of the Disclosure Law and section 40 of the Terrorism Law

APPENDIX F

GUERNSEY STATUTORY INSTRUMENT

2007 No.33

The Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2007[a]

[CONSOLIDATED TEXT]

NOTE

This consolidated version of the enactment incorporates all amendments listed in the footnote below. However, while it is believed to be accurate and up to date, it is not authoritative and has no legal effect, having been prepared in-house for the assistance of the Law Officers. No warranty is given that the text is free of errors and omissions, and no liability is accepted for any loss arising from its use. The authoritative text of the enactment and of the amending instruments may be obtained from Her Majesty's Greffier, Royal Court House, Guernsey, GY1 2PB.

a Amended by Order in Council No. XV of 2008 (Registration of Non-Regulated Financial Services Businesses (Bailiwick of Guernsey) Law, 2008); G.S.I. No. 48 of 2008 (The Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) (Amendment) Regulations, 2008); G.S.I. No. 73 of 2008 (The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 (Amendment of Schedules 1 and 2) Regulations, 2008; and G.S.I. No. 30 of 2009 (The Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) (Amendment) Regulations, 2009); G.S.I. No. 12 of 2010 (The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 (Amendment of Schedules 1 and 2) Regulations, 2010; and G.S.I. No. 13 of 2010 (The Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) (Amendment) Regulations, 2010); G.S.I. No. 58 of 2010 (The Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) (Amendment) (No.2) Regulations, 2010); the Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011 (No. XI of 2011); G.S.I. No.** of 2013 (The Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) (Amendment) Regulations, 2013).

GUERNSEY STATUTORY INSTRUMENT

2007 No.33

The Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2007

ARRANGEMENT OF REGULATIONS

PART IIIA
REQUIREMENT TO REGISTER IN CERTAIN CASES

PART IIIB
DESIGNATION OF SUPERVISORY AUTHORITY

PART IV
MISCELLANEOUS

GUERNSEY STATUTORY INSTRUMENT

2007 No.33

The Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2007

Made	*10th December, 2007*
Coming into operation	*15th December, 2007*
Laid before the States	*30th January, 2008*

THE POLICY COUNCIL, in exercise of the powers conferred upon it by section 49 and 54 of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999[b] and of all other powers enabling it in that behalf, hereby makes the following Regulations:-

PART I

INTRODUCTORY PROVISIONS AND RISK ASSESSMENT

Citation.

1. These Regulations may be cited as the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2007.

Commencement.

2. These Regulations shall come into force on the 15th December, 2007.

---

b Order in Council No. VIII of 1999, as amended by Order in Council No. II of 2005 and No. XV of 2007, Ordinance XXVIII of 1999, Ordinance XII of 2002, G.S.I. No. 27 of 2002 and certain sections of the Law are modified in their application to external confiscation orders by Ordinance XXXIII of 1999.

Risk assessment and mitigation.

3. (1) A financial services business must-

(a) carry out and document a suitable and sufficient money laundering and terrorist financing business risk assessment which is specific to the financial services business-

(i) as soon as reasonably practicable after these Regulations come into force, or

(ii) in the case of a financial services business which only becomes such on or after the date these Regulations come into force, as soon as reasonably practicable after it becomes such a business, and

(b) regularly review its business risk assessment, at a minimum annually, so as to keep it up to date and, where, as a result of that review, changes to the business risk assessment are required, it must make those changes,

(2) A financial services business must-

(a) prior to the establishment of a business relationship or the carrying out of an occasional transaction, undertake a risk assessment of that proposed business relationship or occasional transaction,

(b) regularly review any risk assessment carried out under subparagraph (a) so as to keep it up to date and, where changes to that risk assessment are required, it must make those changes, and

(c) ensure that its policies, procedures and controls on forestalling,

preventing and detecting money laundering and terrorist financing are appropriate and effective, having regard to the assessed risk.

(3) A financial services business must have regard to –

(a) any relevant rules and guidance in the Handbook; and

(b) any notice or instruction issued by the Commission under the Law,

in determining, for the purposes of these Regulations, what constitutes a high or low risk.

PART II

CUSTOMER DUE DILIGENCE ETC.

Customer due diligence.

4. (1) A financial services business shall, subject to the following provisions of these Regulations, ensure that the steps in paragraph (3) are carried out -

(a) when carrying out the activities in paragraphs (2)(a) and (b) and in the circumstances in paragraphs (2)(c) and (d), and

(b) in relation to a business relationship established prior to the coming into force of these Regulations -

(i) in respect of which there is maintained an anonymous account or an account in a fictitious name, as soon as possible after the coming into force of these Regulations and in any event before such account is used again in any way, and

(ii) where it does not fall within subparagraph (i) and to the extent that such steps have not already been carried out, at appropriate times on a risk-sensitive basis.

(2) The activities and circumstances referred to in paragraph (1) are -

(a) establishing a business relationship,

(b) carrying out an occasional transaction,

(c) where the financial services business knows or suspects or has reasonable grounds for knowing or suspecting -

(i) that, notwithstanding any exemptions or thresholds pursuant to these Regulations, any party to a business relationship is engaged in money laundering or terrorist financing, or

(ii) that it is carrying out a transaction on behalf of a person, including a beneficial owner or underlying principal, who is engaged in money laundering or terrorist financing, and

(d) where the financial services business has doubts about the veracity or adequacy of previously obtained identification data.

(3) The steps referred to in paragraph (1) are that -

(a) the customer shall be identified and his identity verified using identification data,

(b) any person purporting to act on behalf of the customer shall be identified and his identity and his authority to so act shall be verified,

(c) the beneficial owner and underlying principal shall be identified and reasonable measures shall be taken to verify such identity using identification data and such measures shall include, in the case of a legal person or legal arrangement, measures to understand the ownership and control structure of the customer,

(d) a determination shall be made as to whether the customer is acting on behalf of another person and, if the customer is so acting, reasonable measures shall be taken to obtain sufficient identification data to identify and verify the identity of that other person,

(e) information shall be obtained on the purpose and intended nature of each business relationship, and

(f) a determination shall be made as to whether the customer, beneficial owner and any underlying principal is a politically exposed person.

(4) A financial services business must have regard to any relevant rules and guidance in the Handbook in determining, for the purposes of this regulation and regulation 5, what constitutes reasonable measures.

Additional customer due diligence.

5. (1) Where a financial services business is required to carry out customer due diligence, it must also carry out enhanced customer due diligence in relation to the following business relationships or occasional transactions -

(a) a business relationship or occasional transaction in which the customer or any beneficial owner or underlying principal is a politically exposed person,

(b) a business relationship which is-

(i) a correspondent banking relationship, or

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

(c) a business relationship or an occasional transaction -

(i) where the customer is established or situated in a country or territory that does not apply or insufficiently applies the Financial Action Task Force Recommendations on Money Laundering, or

(ii) which the financial services business considers to be a high risk relationship, taking into account any notices, instructions or warnings issued from time to time by the Commission, and

(d) a business relationship or an occasional transaction which has been assessed as a high risk relationship pursuant to regulation 3(2)(a).

(2) In paragraph (1) –

(a) "**enhanced customer due diligence**" means

(i) obtaining senior management approval for establishing a business relationship or undertaking an occasional transaction,

(ii) obtaining senior management approval for, in the case of an existing business relationship with a politically exposed person, continuing that relationship,

(iii) taking reasonable measures to establish the source of any funds and of the wealth of the customer and beneficial owner and underlying principal,

(iv) carrying out more frequent and more extensive ongoing monitoring in accordance with regulation 11, and

(v) taking one or more of the following steps as would be appropriate to the particular business relationship or occasional transaction –

(A) obtaining additional identification data,

(B) verifying additional aspects of the customer's identity, and

(C) obtaining additional information to understand the purpose and intended nature of each business relationship.

(b) **"politically exposed person"** means -

(i) 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 including, without limitation -

(A) heads of state or heads of government,

(B) senior politicians and other important officials of political parties,

(C) senior government officials,

(D) senior members of the judiciary,

(E) senior military officers, and

(F) senior executives of state owned body corporates,

(ii) an immediate family member of such a person including, without limitation, a spouse, partner, parent, child, sibling, parent-in-law or grandchild of such a person and in this subparagraph **"partner"** means a person who is considered by the law of the country or territory in which the relevant public function is held as being equivalent to a spouse, or

(iii) a close associate of such a person, including, without limitation -

(A) a person who is widely known to maintain a close business relationship with such a person, or

(B) a person who is in a position to conduct substantial financial transactions on behalf of such a person.

(3) [*Deleted by the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) (Amendment) Regulations, 2009*]

(4) Where the customer was not a Guernsey resident when a financial services business carried out an activity set out in regulation 4(2)(a) or (b), a financial services business must take adequate measures to compensate for the specific risk arising as a result -

(a) when carrying out customer due diligence, and

(b) where the activity was establishing a business relationship, when carrying out monitoring of that relationship pursuant to regulation 11.

Customer due diligence for low risk relationships.

6. (1) Where a financial services business is required to carry out customer due diligence in relation to a business relationship or occasional transaction which has been assessed as a low risk relationship pursuant to regulation 3(2)(a), it may, subject to the following provisions of this regulation -

(a) apply reduced or simplified customer due diligence measures, or

(b) treat an intermediary as if it were the customer.

(2) The discretion in paragraph (1) may only be exercised -

in accordance with the requirements set out in chapter 6 of the Handbook.

(3) For the avoidance of doubt, the discretion in paragraph (1) shall not be exercised -

(a) where the financial services business knows or suspects or has reasonable grounds for knowing or suspecting that any party to a business relationship or any beneficial owner or underlying principal is engaged in money laundering or terrorist financing, or

(b) in relation to business relationships or occasional transactions where the risk is other than low.

Timing of identification and verification.

7. (1) Identification and verification of the identity of any person or legal arrangement pursuant to regulations 4 to 6 must, subject to paragraph (2) and regulation 4(1)(b), be carried out before or during the course of establishing a business relationship or before carrying out an occasional transaction.

(2) Verification of the identity of the customer and of any beneficial owners and underlying principals may be completed following the establishment of a business relationship provided that -

(a) it is completed as soon as reasonably practicable thereafter,

(b) the need to do so is essential not to interrupt the normal conduct of business, and

(c) appropriate and effective policies, procedures and controls are in place which operate so as to manage risk.

Accounts and shell banks.

8. (1) A financial services business must, in relation to all customers-

(a) not set up anonymous accounts or accounts in fictitious names, and

(b) maintain accounts in a manner which facilitates the meeting of the requirements of these Regulations.

(2) A financial services business must -

(a) not enter into, or continue, a correspondent banking relationship with a shell bank, and

(b) take appropriate measures to ensure that it does not enter into, or continue, a correspondent banking relationship where the respondent bank is known to permit its accounts to be used by a shell bank.

(3) In this regulation -

(a) **"consolidated supervision"** means supervision by a regulatory authority of all aspects of the business of a group of bodies corporate carried on worldwide, to ensure compliance with-

(i) the Financial Action Task Force Recommendations on Money Laundering; and

(ii) other international requirements,

and in accordance with the Core Principles of Effective Banking Supervision issued by the Basel Committee on Banking Supervision as revised or reissued from time to time,

(b) **"physical presence"** means the presence of persons involved in a meaningful way in the running and management of the bank which, for the avoidance of doubt, is not satisfied by the presence of a local agent or junior staff, and

(c) **"shell bank"** means a bank that has no physical presence in the country or territory in which it is incorporated and licensed and which is not a member of a group of bodies corporate which is subject to effective consolidated supervision.

Non-compliance with customer due diligence measures etc.

9. Where a financial services business can not comply with any of regulation 4(3)(a) to (d) it must -

(a) in the case of an existing business relationship, terminate that business relationship,

(b) in the case of a proposed business relationship or occasional transaction, not enter into that business relationship or carry out that occasional transaction with the customer, and

(c) consider whether a disclosure must be made pursuant to Part I of the Disclosure Law[c] or section 15 or 15A of the Terrorism Law[d].

---

c Approved by resolution of the States on 30th May 2007.

d Order in Council No. XVI of 2002 as amended by Order in Council No. XIII of 2006 and Ordinance No. XLVI of 2007.

Introduced business.

10. (1) In the circumstances set out in paragraph (2), a financial services business may accept a written confirmation of identity and other matters from an introducer in relation to the requirements of regulation 4(3)(a) to (e) provided that -

(a) the financial services business also requires copies of identification data and any other relevant documentation to be made available by the introducer to the financial services business upon request and without delay, and

(b) the introducer […] keeps such identification data and documents.

(2) The circumstances referred to in paragraph (1) are that the introducer -

(a) is an Appendix C business, or

(b) is either an overseas branch of, or a member of the same group of bodies corporate as, the financial services business with which it is entering into the business relationship (**"receiving financial services business"**), and -

(i) the ultimate parent body corporate of the group of bodies corporate of which both the introducer and the receiving financial services business are members, falls within paragraph (2)(a), and

(ii) the conduct of the introducer 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 on Money Laundering in respect of such a business, and

(iii) the conduct of which is supervised for compliance with the requirements referred to in subparagraph (ii), by the Commission or an overseas regulatory authority.

(3) Notwithstanding paragraph (1), where reliance is placed upon the introducer the responsibility for complying with the relevant provisions of regulation 4 remains with the receiving financial services business.

PART III

ENSURING COMPLIANCE AND RECORD KEEPING

Monitoring transactions and other activity.

11. (1) A financial services business shall perform ongoing and effective monitoring of any existing business relationship, which shall include-

(a) reviewing identification data to ensure it is kept up to date and relevant in particular for high risk relationships or customers in respect of whom there is a high risk,

(b) scrutiny of any transactions or other activity, paying particular attention to all -

(i) complex transactions,

(ii) transactions which are both large and unusual, and

(iii) unusual patterns of transactions,

which have no apparent economic purpose or no apparent lawful purpose, and

(c) ensuring that the way in which identification data is recorded and stored is such as to facilitate the ongoing monitoring of each business relationship.

(2) The extent of any monitoring carried out under this regulation and the frequency at which it is carried out shall be determined on a risk sensitive basis including whether or not the business relationship is a high risk relationship.

Reporting suspicion.

12. A financial services business shall -

(a) appoint a person of at least management level as the money laundering reporting officer and provide the name and title of that person to the Commission and the Financial Intelligence Service as soon as is reasonably practicable and, in any event, within fourteen days starting from the date of that person's appointment,

(b) nominate another person to receive disclosures, under Part I of the Disclosure Law and section 15 of the Terrorism Law ("nominated officer"), in the absence of the money laundering reporting officer, and ensure that any relevant employee is aware of the name of that nominated officer,

(c) ensure that where a relevant employee, other than the money laundering reporting officer, is required to make a disclosure under Part I of the Disclosure Law or section 15 of the Terrorism Law, that this is done by way of a report to the money laundering reporting officer, or, in his absence, to a nominated officer,

(d) ensure that the money laundering reporting officer, or in his absence a nominated officer, in determining whether or not he is

required to make a disclosure under Part I of the Disclosure Law or section 15A of the Terrorism Law, takes into account all relevant information,

(e) ensure that the money laundering reporting officer, or, in his absence, a nominated officer, is given prompt access to any other information which may be of assistance to him in considering any report, and

(f) ensure that it establishes and maintains such other appropriate and effective procedures and controls as are necessary to ensure compliance with requirements to make disclosures under Part I of the Disclosure Law and sections 15 and 15A of the Terrorism Law.

Employee screening and training.

13. (1) A financial services business shall maintain appropriate and effective procedures, when hiring employees, for the purpose of ensuring high standards of employee probity and competence.

(2) A financial services business shall ensure that relevant employees receive comprehensive ongoing training in -

(a) the relevant enactments, these Regulations and the Handbook,

(b) the personal obligations of employees and their potential criminal liability under these Regulations and the relevant enactments,

(c) the implications of non-compliance by employees with any rules, guidance, instructions, notices or other similar instruments made for the purposes of these Regulations, and

(d) its policies, procedures and controls for the purposes of forestalling, preventing and detecting money laundering and terrorist financing.

(3) A financial services business shall identify relevant employees who, in view of their particular responsibilities, should receive additional and ongoing training, appropriate to their roles, in the matters set out in paragraph (2) and must provide such additional training.

Record-keeping.

14. (1) A financial services business shall keep-

(a) a transaction document and any customer due diligence information, or

(b) a copy thereof,

for the minimum retention period.

(2) Where a financial services business is required by any enactment, rule of law or court order to provide a transaction document or any customer due diligence information to any person before the end of the minimum retention period, the financial services business shall-

(a) keep a copy of the transaction document or customer due diligence information until the period has ended or the original is returned, whichever occurs first, and

(b) maintain a register of transaction documents and customer due diligence information so provided.

(3) A financial services business shall also keep records of -

(a) any reports made to a money laundering reporting officer as referred to in regulation 12 and of any disclosure made under Part I of the Disclosure Law or section 15 or 15A of the Terrorism Law made other than by way of a report to the money laundering reporting officer, for five years starting from-

(i) in the case of a report or a disclosure in relation to a business relationship, the date the business relationship ceased, or

(ii) in the case of a report or a disclosure in relation to an occasional transaction, the date that transaction was completed,

(b) any training carried out under regulation 13 for five years starting from the date the training was carried out,

(c) any minutes or other documents prepared pursuant to regulation 15(c) until -

(i) the expiry of a period of five years starting from the date they were finalised, or

(ii) they are superseded by later minutes or other documents prepared under that regulation,

whichever occurs later, and

(d) its policies, procedures and controls which it is required to establish and maintain pursuant to these Regulations, until the

expiry of a period of five years starting from the date that they ceased to be operative.

(4) Documents and customer due diligence information, including any copies thereof, kept under this regulation -

(a) may be kept in any manner or form, provided that they are readily retrievable, and

(b) must be made available promptly –

(i) to an auditor, and

(ii) to any police officer, the Financial Intelligence Service, the Commission or any other person, where such documents or customer due diligence information are requested pursuant to these Regulations or any relevant enactment.

Ensuring compliance, corporate responsibility and related requirements.

15. (1) A financial services business must, in addition to complying with the preceding requirements of these Regulations -

(a) establish such other policies, procedures and controls as may be appropriate and effective for the purposes of forestalling, preventing and detecting money laundering and terrorist financing,

(b) establish and maintain an effective policy, for which responsibility must be taken by the board, for the review of its compliance with the requirements of these Regulations and such policy shall

include provision as to the extent and frequency of such reviews,

(c) ensure that a review of its compliance with these Regulations is discussed and minuted at a meeting of the board at appropriate intervals, and in considering what is appropriate a financial services business must have regard to the risk taking into account -

(i) the size, nature and complexity of the financial services business,

(ii) its customers, products and services, and

(iii) the ways in which it provides those products and services,

(d) subject to paragraph (2) ensure that any of its branch offices and, where it is a body corporate, any body corporate of which it is the majority shareholder, which, in either case, is a financial services business in any country or territory outside the Bailiwick, complies there with -

(i) the requirements of these Regulations, and

(ii) any requirements under the law applicable in that country or territory which are consistent with the Financial Action Task Force Recommendations on Money Laundering,

provided that, where requirements under subparagraphs (i) and (ii) differ, a financial services business must ensure that the requirement which provides the highest standard of compliance, by reference to the Financial Action Task Force Recommendations on Money Laundering, is complied with.

(2) The obligation under paragraph (1)(d) applies to the extent that the law of the relevant country or territory allows and if the law of the that country or territory does not so allow in relation to any requirement of these Regulations, the financial services business must notify the Commission accordingly.

PART IIIA

REQUIREMENT TO REGISTER IN CERTAIN CASES

Application of Part.

15A. This Part applies to those persons who are financial services businesses by virtue of falling within paragraphs 20 to 23 of Part I of Schedule 1 to the Law and who are also financial services businesses by virtue of falling within paragraphs 4 or 5 ("money or value transfer services") or 12 or 13 ("money or currency changing services") of the said Part I.

Requirement to register.

15B. (1) Subject to paragraph (2), a financial services business to which this Part applies must be registered by the Commission for the purposes of this Part.

(2) A financial services business which, immediately prior to the commencement of this Part, is carrying on, and continues to carry on, money or value transfer services or money or currency changing services, shall not, during a period of one month immediately following the commencement of this Part, be guilty of an offence under regulation 17(1) provided that an application for registration in accordance with regulation 15C is submitted before the expiration of that period.

Application for registration.

15C. A financial services business to which this Part applies shall apply to the Commission in such form and manner as the Commission may determine; and such application shall be accompanied by a statement of-

(a) the legal name and any trading names of the applicant,

(b) its principal place of business and any other business addresses in the Bailiwick, and

(c) details of the type of money or value transfer services or money or currency changing services provided.

General requirements.

15D. A financial services business which has been registered under this Part must inform the Commission of any change to the information given to the Commission for the purposes of its application for registration under Regulation 15C, or to any information given to the Commission thereafter –

(a) prior to making such a change, or

(b) where a change is sudden or unexpected, promptly after such change is made,

and for the purposes of this paragraph a change to such information shall include the intention to cease providing money or value transfer services or money currency or changing services.

List of, and information as to, financial services businesses registered under Part IIIA.

15E. (1) The Commission shall –

(a) establish and maintain, in such form as the Commission may determine, a list of all financial services businesses which are for the time being registered under this Part,

(b) make available to any person, on request and on payment of such charge (if any) as the Commission may reasonably demand to cover the cost of preparation, a copy of that list, and

(c) publish a copy of the list on the Commission's official website.

(2) The list maintained under paragraph (1) shall contain, in relation to each financial services business registered under this Part -

(a) a statement of -

(i) the legal name and any trading names of the business,

(ii) its principal place of business and any other business addresses in the Bailiwick, and

(iii) details of the type or types of financial services business falling within paragraph 4 or 5 ("money or value transfer services") or 12 or 13 ("money or currency changing services") by virtue of which it is a financial services business, and

(b) such other particulars as the Commission may determine.

(3) If at any time it appears to the Commission that the list maintained under paragraph (1), or any particular contained in an entry in that list, is, for any reason, inaccurate, the Commission shall make such addition, erasure or other alteration to that list or entry as the Commission considers necessary.

(4) The Commission may give public notice of the fact that a particular financial services business has been registered, or has ceased to be registered, under this Part.

PART IIIB

DESIGNATION OF SUPERVISORY AUTHORITY

Guernsey Financial Services Commission.

15F. (1) The Commission is prescribed as the supervisory authority with responsibility for monitoring and enforcing compliance by financial services businesses with regulations and other measures made or issued under the Law, or any other enactment, for the purpose of forestalling, preventing or detecting money laundering and terrorist financing.

(2) The Commission is also designated as the competent authority–

(a) to register financial service businesses under Part IIIA, and

(b) to register financial businesses under section 2 of the Registration of Non-Regulated Financial Services Businesses (Bailiwick of Guernsey) Law, 2008.

(3) For the purpose of paragraph (1), "measures" includes rules, guidance, instructions, notices and other similar instruments.

PART IV

MISCELLANEOUS

Notification etc.

16. (1) [*Repealed by the Registration of Non-Regulated Financial Services Businesses (Bailiwick of Guernsey) Law, 2008*]

(2) [*Repealed by the Registration of Non-Regulated Financial Services Businesses (Bailiwick of Guernsey) Law, 2008*]

(3) [*Repealed by the Registration of Non-Regulated Financial Services Businesses (Bailiwick of Guernsey) Law, 2008*]

(4) [*Repealed by the Registration of Non-Regulated Financial Services Businesses (Bailiwick of Guernsey) Law, 2008*]

(5) Any person who is a financial services business by virtue of providing money or value transmission services shall maintain a current list of its agents for such services, which shall be made available to the Commission on demand.

Offences as to false and misleading information.

16A. If a person -

(a) in connection with an application for, or for the purposes of obtaining, a registration under Part IIIA of these Regulations,

(b) in purported compliance with a requirement imposed by these Regulations, or

(c) otherwise than as mentioned in paragraph (a) or (b) but in circumstances in which that person intends, or could reasonably be expected to know, that any statement, information or document provided by him would or might be used by the Commission for the purpose of exercising its functions conferred by these Regulations,

does any of the following -

(i) makes a statement which he knows or has reasonable cause to believe to be false, deceptive or misleading in a material particular,

(ii) dishonestly or otherwise, recklessly makes a statement which is false, deceptive or misleading in a material particular,

(iii) produces or furnishes or causes or permits to be produced or furnished any information or document which he knows or has reasonable cause to believe to be false, deceptive or misleading in a material particular, or

(iv) dishonestly or otherwise, recklessly produces or furnishes or recklessly causes or permits to be produced or furnished any information or document which is false, deceptive or misleading in a material particular,

he is guilty of an offence and liable on conviction on indictment, to imprisonment not exceeding a term of five years or a fine or both or on summary conviction, to imprisonment for a term not exceeding 6 months or a fine not exceeding level 5 on the uniform scale or both.

Offences.

17. (1) Any person who contravenes any requirement of these Regulations shall be guilty of an offence and liable -

(a) on conviction on indictment, to imprisonment not exceeding a term of five years or a fine or both,

(b) on summary conviction, to imprisonment for a term not exceeding 6 months or a fine not exceeding level 5 on the Uniform Scale or both.

(2) [*Omitted by The Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) (Amendment) Regulations, 2008*]

(3) [*Omitted by The Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) (Amendment) Regulations, 2008*]

(4) [*Omitted by The Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) (Amendment) Regulations, 2008*]

Amendment to the Law.

18. (1) The Law shall be amended as follows.

(2) For Schedule 1 to the Law substitute the Schedule 1 set out in the Schedule to these Regulations.

Interpretation.

19. (1) In these Regulations, unless the context otherwise requires -

"2002 Regulations" means the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations, 2002,

"account" means a bank account and any other business relationship between a financial services business and a customer which is of a similar nature having regard to the services offered by the financial services business,

"appendix C business" means -

(a) a financial services business supervised by the Commission, or

(b) a business which is carried on from -

(i) a country or territory listed in Appendix C to the Handbook and which would, if it were carried on in the Bailiwick, be a financial services business, or

(ii) the United Kingdom, the Bailiwick of Jersey, the Bailiwick of Guernsey or the Isle of Man by a lawyer or an accountant,

and, in either case, is a business -

(A) which may only be carried on in that

country or territory by a person regulated for that purpose under the law of that country or territory,

(B) the conduct of which is subject to requirements to forestall, prevent and detect money laundering and terrorist financing that are consistent with those in the Financial Action Task Force Recommendations on Money Laundering 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,

"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[e] and related expressions shall be construed accordingly,

"beneficial owner" means, in relation to a business relationship or occasional transaction -

(a) the natural person who ultimately owns or controls the customer, and

[e] No. XIII of 1994 as amended by No. XVII and XXI of 2002, No. XVI of 2003 and [No of 2007 and Guernsey S.I. No. of 2007.]

(b) a person on whose behalf the business relationship or occasional transaction is to be or is being conducted and,

in the case of a foundation or trust or other legal arrangement, this shall mean -

(i) any beneficiary in whom an interest has vested, and

(ii) any other person who benefits from that foundation or trust or other legal arrangement,

"board" means -

(a) the board of directors of a financial services business, where it is a body corporate, or

(b) the senior management of a financial services business, where it is not a body corporate,

"business relationship" means a business, professional or commercial relationship between a financial services business and a customer which is expected by the financial services business, at the time when contact is established, to have an element of duration.

"business risk assessment" means an assessment which documents the exposure of a business to money laundering and terrorist financing 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 (Bailiwick of Guernsey) Law, 1987[f],

"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 financial services business, or

(b) to carry out, or has carried out, an occasional transaction with a financial services 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 financial services business is required to carry out pursuant to regulation 4(3),

"customer due diligence information" means -

(a) identification data, and

(b) any account files and correspondence relating to the business relationship or occasional transaction,

---

f Ordres en Conseil Vol. XXX, p. 243, Orders in Council No. XX of 1991, No. XIII of 1994, No. II of 1997, No. II of 1998 and Nos. XVII and XXI of 2002, No. XXII of 2003 and Ordinance No. XXXIV of 2005.

"Disclosure Law" means the Disclosure (Bailiwick of Guernsey) Law, 2007,

"document" includes information recorded in any form (including, without limitation, in electronic form),

"employee" means an individual working, including on a temporary basis, for a financial services 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" shall be construed in accordance with regulation 5(2)(a),

"Financial Action Task Force Recommendations on Money Laundering" means the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation issued by the Financial Action Task Force as revised or reissued from time to time,

"**Financial Intelligence 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 Investigation Unit**" means that branch of the Customs and Immigration Service responsible for the investigation of financial and economic crime,

"**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,

"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, or

(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 subparagraph (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 subparagraph (a).

"Handbook" means the Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing as revised or re-issued from time to time by the Commission,

"high risk relationship" means a business relationship or an occasional transaction which has a high risk of involving money laundering or terrorist financing and related terms shall be construed accordingly,

"**identification data**" means documents which are from a reliable and independent source,

"**intermediary**" means -

(a) a financial services business, or

(b) a firm of lawyers, or estate agents, operating in Guernsey,

which is considered as being the customer of a financial services business when establishing a business relationship, or undertaking an occasional transaction, in accordance with chapter 6 of the Handbook,

"introducer" means a financial services 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 financial

services business,

"the law" means the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999,

"legal arrangement" means an express trust or any other vehicle whatsoever which has a similar legal effect,

"low risk relationship" means a business relationship or an occasional transaction which has a low risk of involving money laundering or terrorist financing and related terms shall be construed accordingly,

"minimum retention period" means-

(a) in the case of any customer due diligence information -

(i) a period of five years starting from the date-

(A) where the customer has established a business relationship with the financial services business, that relationship ceased,

(B) where the customer has carried out an occasional transaction with the financial services business, that transaction was completed, or

(ii) such other longer period as the Commission may direct,

(b) in the case of a transaction document -

(i) a period of five years starting from the date that both the transaction and any related transaction were completed, or

(ii) such other longer period as the Commission may direct,

"money laundering" is any act which -

(a) constitutes an offence under section 38, 39 or 40 of the Law,

(b) constitutes an offence under section 57, 58 or 59 of the Drug Trafficking (Bailiwick of Guernsey) Law, 2000[g],

(c) constitutes an attempt, conspiracy or incitement to commit an offence specified in paragraph (a) or (b),

(d) constitutes aiding, abetting, counselling or procuring the commission of an offence specified in paragraph (a) or (b), or

(e) would constitute an offence specified in paragraph (a), (b), (c) or (d) if done in the Bailiwick,

irrespective of the value of the property involved and for the purposes of this definition having possession of any property shall be taken to be doing an act in relation to it,

"money laundering reporting officer" means a manager, partner or director -

(a) appointed by a financial services business to have responsibility for compliance with policies, procedures and controls to forestall, prevent and detect money laundering and terrorist financing, and

---

g Order in Council No. VII of 2000 as amended by Order in Council No. II of 2005.

(b) nominated by a financial services business to receive disclosures under Part I of the Disclosure Law and section 15 of the Terrorism Law,

"**notify**" means notify in writing,

"**occasional transaction**" means any transaction involving more than £10,000, carried out by the financial services 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,

"**police officer**" has the meaning in section 51(1) of the Law,

"**politically exposed person**" shall be construed in accordance with regulation 5(2)(b),

"**relevant employees**" means any -

(a) member of the board,

(b) member of the management of the financial services business, and

(c) employees whose duties relate to the financial services business,

"**relevant enactments**" means -

(a) [*Revoked by the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) (Amendment) (No.2) Regulations, 2010*]

(b) [*Revoked by the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) (Amendment) (No.2) Regulations, 2010*]

(c) the Law,

(d) the Drug Trafficking (Bailiwick of Guernsey) Law, 2000,

(e) [*Revoked by the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) (Amendment) (No.2) Regulations, 2010*]

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

(g) the Al-Qaida and Taliban (Freezing of Funds) (Guernsey) Ordinance, 2011,

(h) the Terrorism Law,

(i) the Disclosure Law,

(j) the Transfer of Funds (Guernsey) Ordinance, 2007[h],

(k) the Transfer of Funds (Alderney) Ordinance, 2007[i],

(l) the Transfer of Funds (Sark) Ordinance, 2007,

---

h Ordinance No. XIX of 2007.

i Alderney Ordinance No. of 2007.

(m) the Disclosure (Bailiwick of Guernsey) Regulations, 2007,

(n) the Terrorism and Crime (Bailiwick of Guernsey) Regulations, 2007,

(o) the Registration of Non-Regulated Financial Services Businesses (Bailiwick of Guernsey) Law, 2008,

and such enactments relating to money laundering and terrorist financing as may be enacted from time to time in the Bailiwick,

"risk" means a risk of money laundering or terrorist financing occurring and **"risk assessment"** shall be construed accordingly,

"**subordinate legislation**" means any ordinance, statutory instrument, regulation, rule, order, notice, rule of court, resolution, scheme, warrant, byelaw or other instrument made under any enactment and having legislative effect,

"Terrorism Law" means the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002,

"terrorist financing" means doing any act which -

(a) constitutes an offence under section 8, 9, 10 or 11 of the Terrorism Law, or section 9, 10, 11, 12 or 13 of the Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011, or section 2 or 3 of the Al-Qaida and Taliban (Freezing of Funds) (Guernsey) Ordinance, 2011 and, for the purposes of this definition, the "purposes of terrorism" shall include, to the extent that they do not already do so -

(i) any attempt, conspiracy or incitement to carry out terrorism within the meaning of section 1 of the Terrorism Law, or

(ii) aiding, abetting, counselling or procuring the carrying out of such terrorism,

(b) constitutes an attempt, conspiracy or incitement to commit an offence specified in paragraph (a),

(c) constitutes aiding, abetting, counselling or procuring the commission of an offence specified in paragraph (a), or

(d) would, in the case of an act done otherwise than in the Bailiwick, constitute an offence specified in paragraph (a), (b) or (c) if done in the Bailiwick,

irrespective of the value of the property involved, and for the purposes of this definition having possession of any property shall be taken to be doing an act in relation to it,

"transaction document" means a document which is a record of a transaction carried out by a financial services business with a customer or an introducer,

"underlying principal" means, in relation to a business relationship or occasional transaction, any person who is not a beneficial owner but who-

(a) is a settlor, trustee, protector or enforcer of a trust, or a founder or foundation official of a foundation which is the customer or the beneficiaries of which are the beneficial owners, or

(b) exercises ultimate effective control over the customer or exercises or is to exercise such control over the business relationship or occasional transaction,

and in this definition **"protector"** has the meaning in section 58 of the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc. (Bailiwick of Guernsey) Law, 2000[j].

(2) A 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.

(3) The Interpretation (Guernsey) Law, 1948[k] applies to the interpretation of these Regulations.

NOTES

In section 19, the words in square brackets in subparagraph (a) of the definition of terrorist financing were inserted by the Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011, section 36, Schedule, paragraph 6, with effect from 26th January, 2012.

Revocation.

20. The 2002 Regulations and the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) (Amendment) Regulations, 2006[l] are hereby revoked.

Dated this 10th day of December, 2007

M.W. TORODE
Chief Minister
For and on behalf of the Policy Council

---

j Order in Council No. I of 2001, amended by No. XIV of 2003 and No. XVI of 2007 and Guernsey S.I. No. [ ] of 2007].

k Ordres en Conseil Vol. XIII, p. 355.

l Guernsey S. I. No. 43 of 2006.

SCHEDULE

regulation 18

AMENDMENT TO THE LAW

"SCHEDULE 1[m]

section 49

FINANCIAL SERVICES BUSINESSES

1. The businesses specified in Part I are financial services businesses for the purposes of this Law except where they are incidental or other activities falling within Part II, however, those businesses specified in paragraphs 2 to 18A are only financial services businesses when carried on by way of business for or on behalf of a customer.

PART I

BUSINESSES

2. Lending (including, without limitation, the provision of consumer credit or mortgage credit, factoring with or without recourse, financing of commercial transactions (including forfeiting) and advancing loans against cheques).

3. Financial leasing.

---

m Please note that amendments have been made to this schedule to reflect changes subsequently made to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 by G.S.I. No. 48 of 2008 (The Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) (Amendment) Regulations, 2008); G.S.I. No. 73 of 2008 (The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 (Amendment of Schedules 1 and 2) Regulations, 2008; G.S.I. No. 12 of 2010 (The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 (Amendment of Schedules 1 and 2) Regulations, 2010; and G.S.I. No.** of 2013 (The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) law, 1999 (Amendment of Schedules 1 and 2) Regulations, 2013).

4. Operating a money service business (including, without limitation, a business providing money or value transmission services, currency exchange (bureau de change) and cheque cashing).

4A. Buying, selling or arranging the buying or selling of, or otherwise dealing in, bullion or buying or selling postage stamps, except where –

(a) in the case of buying, selling or arranging the buying or selling of, or otherwise dealing in, bullion, the business consists only of buying, selling or arranging for the buying or selling of bullion, or otherwise dealing in bullion, where the value of each purchase, sale or deal does not exceed £10,000, in total, whether the transaction is executed in a single operation or in two or more operations which appear to be linked,

(b) in the case of buying postage stamps, the business consists only of buying postage stamps where the value of each purchase does not exceed £10,000, in total, whether the transaction is executed in a single operation or in two or more operations which appear to be linked, and

(c) in the case of selling postage stamps, the business consists only of selling postage stamps -

(i) where the value of each sale does not exceed £10,000, in total, whether the transaction is executed in a single operation or in two or more operations which appear to be linked, or

(ii) in the course of -

(A) a postal services business carried on under the

authority of a licence granted under the Post Office (Bailiwick of Guernsey) Law, 2001, or

(B) a business authorized to sell postage stamps by the holder of a licence under that Law.

5. Facilitating or transmitting money or value through an informal money or value transfer system or network.

6. Issuing, redeeming, managing or administering means of payment, means of payment includes, without limitation, credit, charge and debit cards, cheques, travellers' cheques, money orders and bankers' drafts and electronic money.

7. Providing financial guarantees or commitments.

8. Trading (by way of spot, forward, swaps, futures, options, etc.) in -

(a) money market instruments (including, without limitation, cheques, bills and certificates of deposit),

(b) foreign exchange, exchange, interest rate or index instruments, and

(c) commodity futures, transferable securities or other negotiable instruments or financial assets.

9. Participating in securities issues and the provision of financial services related to such issues, including, without limitation, underwriting or placement as agent (whether publicly or privately).

10. Providing settlement or clearing services for financial assets including, without limitation, securities, derivative products or other negotiable instruments.

11. Providing advice to undertakings on capital structure, industrial strategy or related questions, on mergers or the purchase of undertakings, except where the advice is provided in the course of carrying on the business of a lawyer or accountant.

12. Money broking.

13. Money changing.

14. Providing individual or collective portfolio management services or advice.

15. Providing safe custody services.

16. Providing services for the safekeeping or administration of cash or liquid securities on behalf of clients.

17. Carrying on the business of a credit union.

18. Accepting repayable funds other than deposits.

18A. Otherwise investing, administering or managing funds or money on behalf of other persons.

19. [*Omitted by an amendment to Schedule 1 to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as made by the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) (Amendment) Regulations, 2008*]

20. Accepting deposits in the course of carrying on "deposit-taking business" as defined in the Banking Supervision (Bailiwick of Guernsey) Law, 1994.

21. Carrying on "controlled investment business" as defined in the Protection of Investors (Bailiwick of Guernsey) Law, 1987.

22. Carrying on "long term business" as defined in the Insurance Business (Bailiwick of Guernsey) Law, 2002, carrying on business as an "insurance intermediary" in respect of "long term business", both phrases as defined in the Insurance Managers and Insurance Intermediaries (Bailiwick of Guernsey) Law, 2002 or acting as an insurance manager under the authority of a licence under the Insurance Managers and Insurance Intermediaries (Bailiwick of Guernsey) Law, 2002.

23. Carrying on "regulated activities" as defined in the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc. (Bailiwick of Guernsey) Law, 2000, in circumstances where the activity is prohibited except under the authority and in accordance with the conditions of a licence granted by the Commission under section 6 of that Law (a "fiduciary licence"), or carrying on by way of business the activities described in sections 3(1)(g) or (x) of that Law.

PART II

INCIDENTAL AND OTHER ACTIVITIES

24. (1) Any business falling within paragraphs 2 to 18A carried out in the course of carrying on the profession of -

(a) [*Omitted by an amendment to Schedule 1 to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as made by the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) (Amendment) Regulations, 2008*]

(b) [*Omitted by an amendment to Schedule 1 to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as made by the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) (Amendment) Regulations, 2008*]

(c) an actuary where such business is incidental to the provision of actuarial advice or services.

(2) For the purposes of this paragraph, business is incidental to the provision of such advice or services, if -

(a) separate remuneration is not being given for the business as well as for such advice or services,

(b) such advice or services is not itself business falling within paragraphs 2 to 18A, and

(c) the business being carried out is incidental to the main purpose for which that advice or services is provided.

25. The carrying on of any business in Part I -

(a) by way of the provision of in-house legal, accountancy or actuarial advice or services to any business referred to in paragraphs 2 to 23, or

(b) in the course of carrying on the profession (respectively) of a lawyer, accountant or actuary for any client carrying on such a business.

26. [*Repealed by an amendment to Schedule 1 to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as made by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 (Amendment of Schedules 1 and 2) Regulations, 2010*]

27. Activities constituting the restricted activities of dealing, advising and promotion for the purposes of Schedule 2 to the Protection of Investors (Bailiwick of Guernsey) Law, 1987 provided that –

(a) such activities are carried on by a person who is not incorporated or registered in the Bailiwick,

(b) such activities are carried on by a person who does not maintain a physical presence in the Bailiwick,

(c) such activities are carried on from a country or territory listed in Appendix C to the Handbook,

(d) the conduct of such activities 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 on Money Laundering in respect of such activities, and

(e) the conduct of such activities is supervised for compliance with the requirements referred to in item (d), by an overseas regulatory authority.

28. Any business falling within paragraph 22 which is -

(a) carried on by a person who is licensed in the Bailiwick solely to carry on general insurance business under the Insurance Business (Bailiwick of Guernsey) Law, 2002,

(b) carried on by a person who is not incorporated or registered in the Bailiwick,

(c) carried on by a person who does not maintain a physical presence in the Bailiwick,

(d) not managed in or from within the Bailiwick, and

(e) subject to authorisation and supervision by the United Kingdom Financial Services Authority.

29. A business falling within paragraphs 2 to 18A of Part I provided that-

(a) the total turnover of that business, plus that of any other business falling within Part I carried on by the same person, does not exceed £50,000 per annum,

(b) no occasional transactions are carried out in the course of such business, that is to say, any transaction involving more than £10,000, where no business relationship has been proposed or established, including such transactions carried out in a single operation or two or more operations that appear to be linked,

(c) the turnover of such business does not exceed 5% of the total turnover of the person carrying on such business,

(d) the business is ancillary, and directly related, to the main activity of the person carrying on the business,

(e) in the course of such business, money or value is not transmitted or such transmission is not facilitated by any means,

(f) the main activity of the person carrying on the business is not that of a business falling within Part I,

(g) the business is provided only to customers of the main activity of the person carrying on the business and is not offered to the public, and

(h) the business is not carried on by a person who also carries on a business falling within paragraphs 20 to 23 of Part I.".

EXPLANATORY NOTE

(This note is not part of the Regulations)

These Regulations impose requirements on financial services businesses for the purpose of forestalling and preventing money laundering and terrorist financing.

They revoke and replace the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations, 2002 (**"2002 Regulations"**) which also imposed such requirements.

The new Regulations contain significant differences to the 2002 Regulations to reflect revised international recommendations relating to money laundering and terrorist financing.

In particular they contain new obligations relating to carrying out risk assessments in relation to a financial service business as a whole and each business relationship it has with a

customer (regulation 3), more precise requirements relating to the identification of persons on whose behalf transactions are carried out or who have effective control over customers (regulation 4), the timing of customer due diligence (regulation 7), provisions relating to the maintenance of customer accounts and carrying on business with shell banks (regulation 8), the monitoring of business relationships (regulation 11) and ensuring compliance and corporate responsibility for compliance (regulation 15).

The Regulations also substitute the definition of "financial services business" in Schedule 1 to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 (regulation 18 and the Schedule). The main changes of principle to that definition include that there is an express reference to anything that can only lawfully be done by licence or is exempted from that requirement under the Insurance Managers and Insurance Intermediaries (Bailiwick of Guernsey) Law, 2002. The provisions excluding certain incidental and other activities carried on by lawyers, accountants, actuaries and within a group of companies have been reworded and included in a new Part II to the Schedule.

Part I of the Regulations contains the requirements relating to risk assessment, Part II the requirements relating to customer due diligence including where enhanced due diligence must be carried out or where reduced or simplified due diligence may be carried out. Part III contains the requirements on financial services businesses to ensure their compliance with the Regulations, on record keeping and on internal reporting of suspicious transactions and employee training. Part IV provides for offences and penalties and makes similar provision to the 2002 Regulations by requiring specified financial services businesses, not licensed under the main financial services regulatory legislation, to notify certain information to the Guernsey Financial Services Commission; it also contains a new obligation on persons providing money or value transmission services to maintain a list of agents.

A Court must take into account rules and guidance contained in the Guernsey Financial Services Commission's Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing in determining whether a financial services business has complied with these Regulations.

PLEASE NOTE THAT PAGES 229 – 243 HAVE BEEN REPEALED.

THE TRANSFER OF FUNDS (GUERNSEY) ORDINANCE, 2017 CAN BE ACCESSED VIA THE BELOW HYPERLINK:

THE TRANSFER OF FUNDS (GUERNSEY) ORDINANCE, 2017

APPENDIX H

MONEY LAUNDERING AND FINANCING OF TERRORISM TECHNIQUES AND METHODS

What is Money Laundering?

Deception is the heart of money laundering: at its most basic level money laundering is deception by attempting to make assets appear to have been obtained through legal means with legally-earned funds or to be owned by third parties who have no relationship to the true owner.

The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. From the perspective of the criminal, it is no use making a profit from criminal activities if that profit cannot be put to use. A proportion of the profit will often be re-invested into further criminal ventures, but criminals will often wish to use the rest for other purposes. If this activity is to be achieved without being detected the money must be 'laundered'. Money laundering can be described as the processing of criminal proceeds to disguise their illegal origin. Criminals seek to put their proceeds of crime into a state in which it appears to have an entirely respectable origin. If this act is carried out successfully it allows criminals to maintain control over their proceeds and ultimately to provide a legitimate cover for their source of income. Where criminals are allowed to use the proceeds of crime, the ability to launder such proceeds makes crime more attractive.

However, this does not mean that all criminals need to resort to elaborate schemes in order to create the perception of legitimacy of the source and ownership of their assets. Small-time criminals rarely do; they deal in cash and avoid financial institutions as much as possible. Even with regard to larger criminal activities the need to launder money will vary from jurisdiction to jurisdiction.

The money laundering process is generally made up of three stages:

- The placement stage where illegitimate funds find their way into the financial system via payment into legitimate accounts. For example, depositing cash in banks which ask no questions, using business entities that are cash intensive in nature to commingle funds, buying precious metals/diamonds, or artwork/stamp collections;
- The layering stage which is used to disguise the audit trail between the funds and the original point of entry into the financial system. This is achieved by moving the funds around so that the origins of the money become obscured. For example, by transferring funds across borders, purchasing investment bonds, gambling at the race track or at casinos, and making use of foreign financial centres;
- The integration stage where funds are reintroduced as legitimate wealth to fund further activities or to acquire assets.

What is Financing of Terrorism?

For terrorists, the acquisition of funds is not an end in itself but a means of committing a terrorist attack. With terrorist financing, it does not matter whether the transmitted funds come from a legal or illegal source. Indeed, terrorist financing frequently involves funds that, prior to being remitted, are unconnected to any illegal activity. Examples have occurred when legitimate

funds have been donated to charities that, sometimes unknown to the donors, are actually fronts for terrorist organisations.

Tracking terrorist financial transactions arising from legitimate sources is more difficult than following the money trails of the proceeds of crime because of the often relatively small amount of funds required for terrorist actions and the range of legitimate sources and uses of funds. While many organised crime groups are adept at concealing their wealth and cash flows for long periods of time, their involvement in the physical trade of illicit drugs, arms, and other commodities, often exposes the revenues and expenditures connected to these illegal dealings. In contrast, terrorist attacks are in many cases comparatively inexpensive, and their financing is often overshadowed by the larger financial resources allocated for the group's political and social activities, making it more difficult to uncover the illicit nexus.

Identifying and disrupting the mechanisms through which terrorism is financed are key elements in the overall efforts to combat terrorism. As well as reducing the financial flows to terrorists and disrupting their activities, action to counter terrorist financing can provide vital information on terrorists and their networks, which in turn improves law enforcement agencies' ability to undertake successful investigations.

Red Flags

Much of the information in chapter 15 can be used for training purposes and to provide employees with examples of red flags. The case studies below can also be used for training purposes.

Case Studies

The following case studies demonstrate how financial products and services can be used to launder the proceeds of crime or to finance terrorism.

Money Laundering

Example 1 – Laundering through temporary bank accounts

An investigation revealed that the proceeds of a value added tax evasion scheme were laundered through a series of bank accounts established for short term purposes. The launderer transferred the proceeds to a bank and requested that the funds be placed in an account for a short period because he had not decided in which account to place them. A few days later, he instructed the bank to return the money in cash or by cheque. The transaction was not registered in the books of the launderer. Investigators also discovered that the launderer used each bank account for more than one transaction. Afterwards, he sometimes asked the bank to transfer the funds to other accounts at the same bank or another bank, which had been opened on behalf of companies controlled by the launderer. False invoices for fictitious deliveries to these companies were used to justify the transfers.

Example 2 – A PEP launders his proceeds of corruption

A politician and government official in Country M arranged for his wife and children to receive the benefits of payments for infrastructure projects ranging from public swimming pools to power stations which he had supported on receipt of substantial payments.
Trusts and companies were established in a number of tax neutral countries for each of the family members.

A large proportion of the family's wealth – some of which was inherited – was administered by a bank in Country M. The bank had made introductions to the service providers in the tax neutral countries. In addition, the politician entered into business ventures in other jurisdictions, particularly Country L, a European country with a sophisticated finance sector. In all his transactions in foreign countries the politician portrayed himself as a businessman.

As a change in government in Country M became likely the politician asked the local bank to arrange for the administration of much of the family's portfolio to be moved to a bank in Country L. It was only when newspaper reports of the corrupt practices in Country M enabled the bank in Country L to make enquiries and to draw a link between the politician in Country M and the assets it administered that a disclosure report was made to the Financial Intelligence Unit (FIU).

Example 3 – A trust structure and loans are used for laundering the proceeds of alcohol smuggling

A national of Country A was convicted of smuggling a huge quantity of alcohol. A small part of the proceeds were confiscated. The police found documents showing a company in Country A had mortgage loans from a company owned by a trust in Country B. After the conviction, the FIU in Country A learned that the convicted person and his common law wife were the beneficial owners of the company in Country A. With assistance from the office of the public prosecutor in Country B, the FIU obtained information which showed that the company received money from a bank account in a third country (Country C). It was suspected that the proceeds from the smuggling had been transported as cash to the Country C bank, the funds were then transferred to the company owned by the trust in Country B and finally remitted back to Country A as "mortgage loans". It was clear that neither the companies, nor the convicted person, nor his common law wife had paid any instalments on the mortgage.

Example 4 – A lawyer uses cross-border companies and trust accounts to launder money

Mr S headed an organisation importing narcotics into Country A from Country B. A lawyer, Mr L, was employed by Mr S to launder the proceeds of this operation.

In order to launder the proceeds of the narcotics operation, Mr L established a web of foreign corporate entities. These entities were incorporated in Country C, where scrutiny of ownership, records, and finances was not strong. A local management company in Country D administered these companies. The companies were used to camouflage the movement of illicit funds, the acquisition of assets and the financing of criminal activities. Mr S was the holder of 100% of the bearer share capital of these entities.

In Country A, a distinct group of persons and companies without any apparent association to Mr S transferred large amounts of money to Country D where it was deposited in, or transited through, the companies owned by Mr S. This same network was found to have been used to transfer large amounts of money to a person in Country E who was later found to be responsible for drug shipments destined for Country A.

Several other lawyers and their client accounts were found to have been used to receive cash and transfer funds, ostensibly for the benefit of commercial customers in Country A.

Concurrently, Mr L established a separate similar network (which included other lawyers) to purchase assets and place funds in vehicles and instruments designed to mask the beneficial owner's identity.

Example 5 – Bull markets provide laundering opportunity

The equity market in Country C was in a bull phase. An individual who claimed he was a wealthy property developer from Country D approached an investment adviser in country C. He stressed that he wished to invest in equities as quickly as possible. A portfolio was purchased and after several months the individual closed his positions, claiming that he anticipated the bull market would shortly enter a bear phase. Just before payment the individual inexplicably arranged for funds to be transmitted to the account of a company in Country G. The investment adviser made a disclosure report to the FIU.

Example 6 – A securities firm is compromised by fraud and tainted funds

A securities professional opened an account in the name of the wife of his customer and deposited the proceeds of a legitimate real estate sale. He then engaged in a series of fraudulent put and call transactions on behalf of his customer, fabricating contracts after the price trends of the underlying securities were known. The contracts were designated as a put or a call based on the established price trend of the security, so as to ensure in every case that his client would realise a profit. Through this process, the professional was able to introduce over US$157,000 representing the proceeds of crime into his customer's account and to justify its presence as profit from derivatives transactions.

Example 7 – Insurance policies and real estate

An insurance company in country A reported a disclosure to the FIU that it had underwritten two life insurance policies with a total value of US $268,000 in the name of two European nationals. Payment was made by a cheque drawn on the accounts of a brokerage firm in a major, foreign EU financial market and a notary in the south-eastern region of the country. The two policies were then put up as collateral for a mortgage valued at US$1,783,000 that was provided by a company specialising in leasing transactions. As the policyholders did not make payment in their own names, the insurance company contacted the brokerage firm in order to discover the exact origin of the funds deposited in its account. It was informed that the funds had been received in cash and that the parties concerned were merely occasional clients. The case was passed to the prosecution authorities.

APPENDIX H (CONTINUED)

Example 8 – Money launderers use insurance intermediaries to "clean" their funds

Money launderers in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the customers by way of an identification card,

but these details were unable to be clarified by the providing institution locally, which relied on the intermediary doing customer due diligence checks.

The policies were put in place and the relevant payments made by the intermediary to the local insurer. After a couple of months had elapsed, the insurer would receive notification from the customer stating that there was now a change in circumstances, and he/she would have to close the policy. The money launderers suffered losses but came away with "clean" cheques from the local insurer.

On other occasions a policy would be left to run for a couple of years before being closed with the request that the payment be made to a third party. This was often paid, with the receiving institution, if local, not querying the payment as it had come from another reputable local institution.

Example 9 – Foreign exchange transaction leads to case of laundered drug and diamond smuggling proceeds

A foreign exchange transaction of euro into US dollars for a value of almost US$177,000 was reported to the FIU of Country A. At the time of the transaction, the individual gave the exchange office an address in another country (Country B). This first transaction was soon followed by four more similar transactions. After several weeks, the total value of the transactions reached US$618,000. After a break of six months, the transactions resumed. Over a four month period, the individual reappeared with further large amounts of euro to be converted into dollars. The total amount of the transactions described in disclosure reports to the FIU amounted to more than US$1.3 million.

The information obtained by law enforcement authorities indicated that the individual had no criminal record in Country A. As the case involved large amounts, for which there existed no apparently legitimate economic justification, the FIU pursued the investigation. Several foreign FIUs were approached. One of them (in Country F) was able to provide useful information: the individual was known as a member of a group of drug traffickers which performed the same type of foreign transactions in Country F. Investigations of the members of this group were already in progress in Country F. It also appeared that the address provided by the individual during the first contact with the bureau de change in Country A was false. On the basis of these elements, the FIU decided to turn over the case file to the prosecution authority.

The investigation showed that the individual had not been acting alone. For a number of years she had played a dominant role in money laundering transactions involving a total amount of around US$11.5 million. The individual was arrested in the company of one of her accomplices and in possession of a large sum in US dollars. She acknowledged the foreign exchange transactions, as well as the illicit origin of the funds from illegal diamond trafficking.

She was sentenced to four years in prison (two of which were suspended) and a fine of nearly US$1 million. The funds seized were confiscated.

Example 10 – Payments are structured via a money remitter to avoid detection

Over a four year period, Mr A and his uncle operated a money remittance service known as Company S and conducted their business as an agent of a larger money remitting business that was suspected of being used to finance terrorism. An investigation was initiated in relation to Company S based on a disclosure report.

The investigation showed that over the four year period, Mr A's business had received over US$4 million in cash from individuals wishing to transmit money to various countries. When Mr A's business received the cash from customers, it was deposited into multiple accounts at various branches of banks in Country G. In order to avoid the automatic financial reporting requirements in effect in Country G, Mr A and others always deposited the cash with the banks in sums of less than US$10,000, sometimes making multiple deposits of less than US$10,000 in a single day.

Mr A was charged and pleaded guilty to a conspiracy to structure currency transactions in order to evade financial reporting requirements.

Example 11 – US$178 million is laundered through internet gambling scheme and leasing arrangements

A joint investigation by the national criminal and fiscal police of Country C targeted a sports tout service (STC) providing its illegal gambling services by means of the internet. The STC also functioned as an internet service provider (ISP). The STC collected, collated, and analysed statistical and other information relative to sporting events, and then sold this information to subscribers who would factor it into their betting decisions. The targeted STC/ISP expanded its services to include two gambling operations located in Countries D and E, both of which accepted wagers via the internet or toll-free telephone numbers. Police agents were successful in infiltrating the targeted operation.

To launder the proceeds from their illegal internet gambling activities, the subjects of the investigation employed the services of a lawyer. He devised an elaborate scheme using leasing arrangements to which the STC/ISP was party and bank accounts in Countries D and E. Funds were eventually funnelled back to banks in Country C. Investigators estimate that approximately US$178 million was wagered through the STC/ISP annually.

Subjects in this investigation are potentially open to charges of gambling, money laundering, tax evasion and other organised crime related offences.

Example 12 – Property, equities and artworks

The FIU of Country G received information that a previously convicted drug trafficker had made several investments in real estate and was planning to buy a hotel. An assessment of his financial situation did not reveal any legal source of income, and he was subsequently arrested and charged with an offence of money laundering. Further investigation substantiated the

charge that part of the invested funds were proceeds of his own drug trafficking. He was charged with drug trafficking, drug money laundering and other offences.

The criminal's lawyer received the equivalent of approximately US$70,000 cash from his client, placed this money in his client's bank account and later made investments in equity products on the customer's instructions. He was convicted of money laundering in relation to these transactions. Another part of the drug proceeds was laundered by a director of an art museum in a foreign country who received US$15,000 for producing forged documents for the sale of artworks which never took place.

Terrorist Financing

Example 1 – An individual's account activity and inclusion on an official list show possible link to terrorist activity

An individual residing in Country A had a demand deposit account and a savings account at a bank in Country B. The bank that maintained the accounts noticed the gradual withdrawal of funds from the accounts and decided to monitor the accounts more closely. The suspicions of the bank were subsequently reinforced when a name very similar to that of the account holder appeared in an official list of persons and/of entities suspected of involvement in terrorism. The bank immediately made a report to the FIU.

The FIU analysed the financial movements relating to the accounts of the individual using records requested from the bank. Both of the accounts had been opened by the individual in 1990 and had been fed mostly by cash deposits.

The individual made a sizeable transfer from his savings account to his demand deposit account. These funds were used to pay for a single premium life insurance policy and to purchase certificates of deposit. The individual made several more large transfers from his savings account to his demand deposit account. These funds were transferred abroad to persons and companies located in neighbouring countries and in other regions. The individual then sold the certificates of deposit and transferred the profits to the accounts of companies based in Asia and to that of a company established in his country of origin.

The FIU made enquiries internationally. The anti-money laundering unit in the individual's country of origin communicated information related to suspicious operations carried out by the individual and by the companies that received the transfers. This enabled the FIU to draw links between the individual, the companies and money laundering and terrorist financing.

Example 2 – Cash deposits to the accounts of a non-profit organisation are used to finance terrorist group

The FIU in Country L received a disclosure report from a bank regarding an account held by an investment company in another jurisdiction. The bank's suspicions had arisen after the company's secretary made several large cash deposits in different foreign currencies. According to the secretary these funds were intended to finance companies in the media sector. The FIU requested information from several financial institutions. Through these enquiries, it learned that the directors of the investment company were residing in Country L and a bordering

country. They had opened accounts at various banks in Country L under the names of media companies and a non-profit organisation involved in the promotion of cultural activities.

According to the analysis by the FIU, the directors of the investment company and several other customers had made cash deposits to the accounts. These funds were ostensibly intended for the financing of media based projects. The analysis further revealed that the account held by the non-profit organisation was receiving almost daily deposits in small amounts from third parties. The manager of this organisation stated that the money deposited in this account originated from its members for the funding of cultural activities.
Police information obtained by the FIU revealed that the directors of the investment company were known to have been involved in money laundering and that an investigation was already under way into their activities. The directors appeared to be members of a terrorist group, which was financed by extortion and narcotics trafficking. Funds were collected through the non-profit organisation.

Example 3 – Loans for hotels for individuals with suspected terrorist links revealed by a disclosure report

The FIU in Country D received a disclosure report from a domestic bank regarding an account held by an individual residing in a neighbouring country. The individual managed European-based companies and had filed two loan applications on their behalf with the reporting institution. These loan applications amounted to several million US dollars and were ostensibly intended for the purchase of luxury hotels in Country D. The bank did not grant any of the loans.

The analysis by the FIU revealed that the funds for the purchase of the hotels were to be channelled through the accounts of the companies represented by the individual. One of the companies making the purchase of these hotels would then have been taken over by an individual from another country. This second person represented a group of enterprises whose activities focused on the hotel and leisure sectors, and he appeared to be the ultimate intended buyer of the hotels. On the basis of the analysis by the FIU, it appeared that the subject of the disclosure report was acting as a front for the ultimate intended buyer. The latter individual, as well as his family, were suspected of being linked to terrorism.

Example 4 – Fake car accident and life insurance to be used to fund terrorism

Intelligence sources in Country G uncovered information that a member of a suspected terrorist cell was purchasing life insurance policies from a large number of insurers. The intelligence sources were also aware that the individual intended to visit a country in another region where his death was to be faked in a car accident – his wife was to collect the insurance, which was to be used to fund terrorism. Members of the cell were arrested when it was discovered that they intended to move their base of operations from Country G to another country.

APPENDIX I

LINKS TO USEFUL WEBSITE ADDRESSES

Selection of the link listed below will take you to the corresponding website.

Links to official sites in Guernsey

Guernsey Financial Services Commission
Guernsey Finance
Guernsey Financial Intelligence Service
States of Guernsey

Links to other official sites

Asia/Pacific Group on Money Laundering
Basel Committee for Banking Supervision
British Bankers Association
Caribbean Financial Action Task Force (CFATF)
Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL)
Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
Eurasian Group (EAG)
European Parliament
Financial Action Task Force
Financial Action Task Force on Money Laundering in South America (GAFISUD)
Group of States against Corruption
HM Treasury
HM Treasury – Asset Freezing Unit
Intergovernmental Action Group against Money-Laundering in Africa (GIABA)
International Association of Insurance Fraud Agencies, Inc
International Association of Insurance Supervisors
International Monetary Fund
International Organization of Securities Commissions
Interpol
Isle of Man Financial Supervision Commission
Isle of Man Insurance and Pensions Authority
Jersey Financial Services Commission
Middle East and North Africa Financial Action Task Force (MENAFATF)
Offshore Group of Banking Supervisors
Offshore Group of Insurance Supervisors
Organisation for Economic Cooperation and Development
Transparency International Corruption Perception Index
UK Financial Services Authority
UK Foreign and Commonwealth Office
UK Joint Money Laundering Steering Group
UK Office of Public Sector Information
UK Serious Organised Crime Authority
United Nations
United Nations – Office on Drugs and Crime (UNODC)
World Bank

APPENDIX J

PROJET DE LOI

ENTITLED

The Prevention of Corruption (Bailiwick of Guernsey) Law, 2003

ARRANGEMENT OF SECTIONS

PROJET DE LOI

ENTITLED

The Prevention of Corruption (Bailiwick of Guernsey) Law, 2003

THE STATES, in pursuance of their Resolution of the 1st day of November 2001[a], have approved the following provisions which, subject to the Sanction of Her Most Excellent Majesty in Council, shall have force of law in the Bailiwick of Guernsey.

Corrupt transaction with agents.

1. (1) An agent or any other person who corruptly -

(a) accepts or obtains; or

(b) agrees to accept or attempts to obtain,

for himself, or for any other person, any gift, consideration or advantage as an inducement to, or reward for, or otherwise on account of, the agent doing any act or making any omission in relation to his office or position or his principal's affairs or business shall be guilty of an offence.

(2) A person who corruptly -

(a) gives or agrees to give, or

(b) offers,

[a] Article XXI of Billet d'État No. XXI of 2001.

any gift, consideration or advantage to an agent or any other person, whether for the benefit of that agent, person or other person, as an inducement to, or reward for, or otherwise on account of, the agent doing any act or making any omission in relation to his office or position or his principal's affairs or business shall be guilty of an offence.

(3) For the purposes of this section it is immaterial if -

(a) the principal's affairs or business have no connection with the Bailiwick and are conducted in a country or territory outside the Bailiwick;

(b) the agent's functions have no connection with the Bailiwick and are carried out in a country outside the Bailiwick.

(4) A person guilty of an offence under this section shall be liable-

(a) on summary conviction, to imprisonment for a term not exceeding 12 months, to a fine not exceeding level 5 on the uniform scale, or to both; or

(b) on conviction on indictment, to imprisonment for a term not exceeding 7 years, to a fine, or to both.

(5) In this section -

"consideration" includes valuable consideration of any kind;

"principal" includes any employer.

Meaning of "agent".

2. (1) In this Law -

"agent" includes -

(a) any person employed by or acting for another,

(b) without prejudice to the generality of paragraph (a), a person of any of the following descriptions -

(i) a member of the States of Guernsey, the States of Alderney or the Chief Pleas of Sark,

(ii) the Bailiff, the Deputy Bailiff or a Lieutenant Bailiff,

(iii) a Judge of the Court of Appeal,

(iv) a Jurat of the Royal Court,

(v) the Magistrate or Assistant Magistrates,

(vi) a Jurat of the Court of Alderney,

(vii) a member of any tribunal created by or under any enactment of the Bailiwick or any part thereof,

(viii) the Seneschal of Sark or his Deputy,

(ix) Her Majesty's Procureur and any Procureur délégué,

(x) Her Majesty's Comptroller and any Contrôle délégué,

(xi) Her Majesty's Greffier and his Deputies,

(xii) Her Majesty's Sheriff and his Deputies,

(xiii) Her Majesty's Sergeant and his Deputies,

(xvi) the Clerk of the Court of Alderney,

(xv) the Greffier of Sark or his Deputy,

(xvi) the Prevôt of Sark or his Deputy,

(xvii) the Constable and Vingtenier of Sark;

(xviii) a person elected to Parochial office in Guernsey;

(xix) a member of a Parish Douzaine;

(xx) an auditor;

(xxi) a non States member of a States' Committee;

(xxii) a member of any body created by or under any enactment responsible for the regulation of any type of business or other activity,

(xxiii) any other person employed by or acting on behalf of the public administration in any part of the Bailiwick, and

(c) without prejudice to the generality of paragraph (a), a person of any of the following descriptions -

(i) a member of the government of any other country or territory,

(ii) a member of a parliament, regional or national, of any

other country or territory,

(iii) a member of the European Parliament,

(iv) a member of the Court of Auditors of the European Communities,

(v) a member of the Commission of the European Communities,

(vi) a public prosecutor in any other country or territory,

(vii) a Judge of a court in any other country or territory,

(viii) a Judge of any court established under an international agreement,

(ix) a member of, or any other person employed by or acting for or on behalf of, any body established under an international agreement,

(x) a member of a body created by law in any other country or territory responsible for the regulation of any type of business or other activity, and

(xi) any other person employed by or acting on behalf of the public administration of any other country or territory.

(2) The States by Ordinance may amend subsection (1).

Corruption by public officials.

3. (1) A public official who does or does not do any act in relation to his office for the purpose of corruptly obtaining a gift, consideration or advantage for himself or any other person shall be guilty of an offence.

(2) A person guilty of an offence under this section shall be liable-

(a) on summary conviction, to imprisonment for a term not exceeding 12 months, to a fine not exceeding level 5 on the uniform scale, or to both; or

(b) on conviction on indictment, to imprisonment for a term not exceeding 7 years, to a fine, or to both.

(3) In this section -

"**consideration**" includes valuable consideration of any kind;

"**public official**" means a person referred to in section 2(1)(b).

Corruption committed outside the Bailiwick.

4. (1) This section applies if -

(a) a Bailiwick person or a body incorporated under the law of any part of the Bailiwick does or omits to do anything in a country or territory outside the Bailiwick, and

(b) the act or omission would, if done in the Bailiwick, constitute any offence under this Law.

(2) In such a case -

(a) the act or omission constitutes the offence concerned, and

(b) proceedings for the offence may be taken in the Bailiwick.

(3) A "**Bailiwick person**" means a person who is an agent by reason of section 2(1)(b) or any other person who is ordinarily resident in the Bailiwick and who is -

(a) a British citizen, a British Dependent Territories citizen, a British National (Overseas) or a British Overseas citizen,

(b) a person who under the British Nationality Act 1981 is a British subject, or

(c) a British protected person within the meaning of that Act.

Corruption occurring partially in the Bailiwick.

5. A person may be tried in the Bailiwick for an offence under sections 1 or 3, if any of the acts or omissions alleged to constitute the offence was committed in the Bailiwick notwithstanding that other acts or omissions constituting the offence were committed outside the Bailiwick.

Offences by bodies corporate.

6. (1) Where an offence under this Law is committed by a body corporate and is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, any director, manager, secretary or other officer of the body corporate or any person purporting to act in any such capacity, he as well as the body corporate is guilty of the offence and may be proceeded against and punished accordingly.

(2) Where the affairs of a body corporate are managed by its members, subsection (1) shall apply in relation to the acts and defaults of a member in connection with his functions of management as if he were a director or manager of the body corporate.

Search warrants.

7. (1) The Bailiff or appropriate judicial officer on hearing evidence on oath from a police officer may, if he is satisfied that there are reasonable grounds for suspecting that evidence of or relating to the commission of an offence under this Law ("an offence") is to be found in any place, issue a warrant for the search of any premises and any persons found on those premises.

(2) A warrant issued under this section shall authorise police officers and any other persons named in the warrant to enter within one calendar month of the date of issue of the warrant, using if necessary reasonable force, the premises named in the warrant, and to search them and any persons found on them and to seize anything found in the possession of a person present at the time of the search which a police officer involved in conducting the search reasonably believes to be evidence of or relating to the commission of an offence or suspected offence.

(3) A police officer acting under the authority of a warrant under this section may -

(a) require any person present at the place where the search is being carried out to give to the police officer his name and address, and

(b) arrest without warrant any person who -

(i) obstructs or attempts to obstruct a police officer in the carrying out of his duties,

(ii) fails to comply with a requirement under paragraph (a), or

(iii) gives a name or address which the police officer has reasonable cause for believing is false or misleading.

(4) A person who obstructs or attempts to obstruct a police officer acting under the authority of a warrant issued under this section, fails to comply with a requirement

under subsection (3)(a), or gives a false or misleading name or address to a police officer so acting shall be guilty of an offence and shall be liable on summary conviction to imprisonment for a period not exceeding 6 months, to a fine not exceeding level 5 on the uniform scale, or to both.

(5) The power to issue a warrant under this section is without prejudice to any other power conferred by statute for the issue of a warrant for the search of any place or person.

(6) No application for a warrant under this section may be made without the consent of Her Majesty's Procureur.

Interpretation.

8. (1) In this Law -

"agent" has the meaning given by section 2,

"appropriate judicial officer" means -

(a) in Alderney, the Chairman of the Court of Alderney or, if he is absent or unable to act, a Jurat of the Court of Alderney authorised by him to act in that behalf,

(b) in Sark, the Seneschal or, if he is absent or unable to act, his deputy,

"**Bailiwick**" means the Bailiwick of Guernsey,

"Bailiwick person" has the meaning given in section 4(4),

"Her Majesty's Procureur" save for in section 2(1)(b) includes Her Majesty's Comptroller,

"**police officer**" means -

(a) in relation to Guernsey, Herm and Jethou, a member of the salaried police force of the Island of Guernsey and, within the limits of his jurisdiction, a member of the special constabulary of the Island of Guernsey,

(b) in relation to Alderney, a member of the said salaried police force, a member of any police force which may be established by the States of Alderney and, within the limits of his jurisdiction, a member of the Alderney Special Constabulary established pursuant to section 46A of the Government of Alderney Law, 1987[b],

(c) in relation to Sark, the Constable, the Vingtenier and a member of the said police force of the Island of Guernsey, and

(d) an officer within the meaning of section 1(1) of the Customs and Excise (General Provisions) (Bailiwick of Guernsey) Law, 1972[c].

(2) The provisions of the Interpretation (Guernsey) Law, 1948[d] shall apply to the interpretation of this Law throughout the Bailiwick.

(3) Any reference in this Law to an enactment is a reference thereto as from time to time amended, replaced or re-enacted (in either case, with or without modification), extended or applied.

---

b Ordres en Conseil Vol. XXX, p.37, Vol. XXXI, pp.83 and 306; Order in Council No. XI of 1993; No. IX of 1995; No. IV of 1996; No. IV of 1998; and No. I of 2000.

c Ordres en Conseil Vol. XXIII, p.573 and No. XIII of 1991.

d Ordres en Conseil Vol. XIII, p.355.

Common law bribery.

9. The common law offence of bribery is abolished.

Repeal.

10. The Corruption (Alderney) Law, 1994[e] is repealed.

Citation.

11. This Law may be cited as the Prevention of Corruption (Bailiwick of Guernsey) Law, 2003.

---

[e] Order in Council No. XXXI of 1994.

APPENDIX K

PROJET DE LOI

ENTITLED

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

ARRANGEMENT OF SECTIONS

PROJET DE LOI

ENTITLED

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

THE STATES, in pursuance of their Resolution of the 30th March, 2011[f], have approved the following provisions which, subject to the Sanction of Her Most Excellent Majesty in Council, shall have force of law in the Bailiwick of Guernsey.

PART I
DESIGNATIONS

Meaning of "designated person".

1. In this Law, "**designated person**" means –

(a) a person who is the subject of a designation under this Law,

(b) a person who is the subject of a designation under and within the meaning of the Terrorist Asset-Freezing etc. Act 2010[g], or

(c) a natural or legal person, group or entity included in the list provided for by Article 2(3) of Council Regulation (EC) No 2580/2001 of the 27th December 2001[h] on specific restrictive measures directed against certain persons and entities with a view to combating terrorism (as that Regulation is amended from time to time).

Interim designation.

2. (1) The Policy Council may make an interim designation of a person if –

(a) the Policy Council reasonably suspects –

(i) that the person is or has been involved in terrorist activity,

---

f Article V of Billet d'Etat No. IV of 2011.
g An Act of Parliament (2010 c.38).
h OJ L 344, 28.12.2001, p. 70.

(ii) that the person is owned or controlled directly or indirectly by a person within subparagraph (i), or

(iii) that the person is acting on behalf of or at the direction of a person within subparagraph (i), and

(b) the Policy Council considers that it is necessary for purposes connected with protecting members of the public from terrorism that financial restrictions should be applied in relation to the person.

(2) Sections 4(2) to (4) apply for the purposes of this section as they apply for the purposes of Section 4.

(3) The Policy Council may not make more than one interim designation of the same person in relation to the same, or substantially the same, evidence.

(4) Nothing in this section prevents the making of a final designation in accordance with section 4 of a person who has been the subject of an interim designation.

Duration of interim designation.

3. (1) An interim designation of a person –

(a) is of no effect during any period when the person is a designated person under section 1(b) or (c), and

(b) expires at the end of the 30 days beginning with the day on which it was made, or when a final designation of the person is made, whichever is earlier.

(2) Where an interim designation expires the Policy Council must –

(a) give written notice of the expiry to the designated person, and

(b) take reasonable steps to bring the expiry to the attention of the persons who were informed of the designation.

(3) Where an interim designation expires on the making of a final designation in relation to the same person –

(a) a notice under subsection (2) may be combined with written notice under section 6 of the final designation, and

(b) steps under subsection (2) may be combined with steps under section 6 to publicize the final designation.

Power to make final designation.

4. (1) The Policy Council may make a final designation of a person if –

(a) the Policy Council believes –

(i) that the person is or has been involved in terrorist activity,

(ii) that the person is owned or controlled directly or indirectly by a person within subparagraph (i), or

(iii) that the person is acting on behalf of or at the direction of a person within subparagraph (i), and

(b) the Policy Council considers that it is necessary for purposes connected with protecting members of the public from terrorism that financial restrictions should be applied in relation to the person.

(2) For the purposes of this section, involvement in terrorist activity is any one or more of the following –

(a) the commission, preparation or instigation of acts of terrorism,

(b) conduct that facilitates the commission, preparation or instigation of such acts, or that is intended to do so, and

(c) conduct that gives support or assistance to persons who are known or believed by the person giving the support or assistance to be involved in conduct falling within paragraph (a) or (b).

(3) For the purposes of this section, it is immaterial whether the acts of terrorism in question are specific acts of terrorism or acts of terrorism generally.

(4) The reference in subsection (1)(b) to financial restrictions includes a reference to restrictions relating to economic resources.

Duration and renewal of final designation.

5. (1) A final designation of a person –

(a) is of no effect during any period when the person is a designated person under section 1(b) or (c), and

b) expires 12 months after it was made, unless it is renewed.

(2) The Policy Council may renew a final designation of a person at any time before it expires, if the requirements for final designation under section 4 are met in respect of the person at the time of the renewal.

(3) A final designation so renewed expires 12 months after it was renewed (or last renewed), unless it is renewed again.

(4) Section 6 applies to the renewal under this section of a final designation in the same way as it applies to a final designation under section 4.

(5) Where a final designation expires the Policy Council must –

(a) give written notice of the expiry to the designated person, and

(b) take reasonable steps to bring the expiry to the attention of the persons who were informed of the designation.

(6) Nothing in this section prevents the Policy Council from designating a person more than once under section 4.

Notification of designation.

6. (1) Where the Policy Council makes a designation of a person, the Policy Council must –

(a) give written notice of the designation to the person, and

(b) take steps to publicize the designation.

(2) Unless one or more of the following conditions is satisfied, the Policy Council must take steps to publicize the designation generally –

(a) the Policy Council believes that the designated person is an individual under the age of 18,

(b) the Policy Council considers that disclosure of the designation should be restricted –

(i) in the interests of the security of the Bailiwick or of any other country or territory,

(ii) for reasons connected with the prevention or detection of serious crime, or

(iii) in the interests of justice.

(3) If one or more of those conditions is satisfied, the Policy Council must inform only such persons of the designation as the Policy Council considers appropriate.

(4) If one or more of the conditions referred to in subsection (2) is satisfied in respect of a designation, but later none of the conditions referred to in subsection (2) is satisfied in respect of the designation, and the designation is still in effect, the Policy Council must –

(a) give written notice of that fact to the designated person, and

(b) take steps to publicize the designation generally.

Variation or revocation of designation.

7. (1) The Policy Council may at any time vary or revoke a designation.

(2) Where the Policy Council varies or revokes a designation of a person, the Policy Council must –

(a) give written notice of the variation or revocation to the person, and

(b) take reasonable steps to bring the variation or revocation to the attention of the persons who were informed of the designation under section 6.

(3) If the Policy Council refuses an application by a person for the variation or revocation of the person's designation by the Policy Council, the Policy Council must give written notice of the refusal to the person.

Confidential information.

8. (1) Where the Policy Council in accordance with section 6(3) informs only certain persons of the designation of a person, the Policy Council may specify that the information conveyed in so informing those people is to be treated as confidential.

(2) A person who –

(a) is provided with information that is so specified as to be treated as confidential, or

(b) obtains such information, must not disclose it if the person knows, or has reasonable cause to suspect, that the information has been specified under subsection (1) as information to be treated as confidential.

(3) Subsection (2) does not apply to any disclosure made by the person if that disclosure is made with lawful authority.

(4) For the purposes of subsection (3), information is disclosed with lawful authority only if and to the extent that –

(a) the disclosure is made by the Policy Council or authorized by the Policy Council,

(b) the disclosure is made by the designated person or made with the consent of the designated person,

(c) the disclosure is necessary to give effect to a requirement imposed under or by virtue of this Law or any other enactment, or

(d) the disclosure is required by any direction or order of the Royal Court.

(5) This section does not prevent the disclosure of information that is already, or has previously been, available to the public from other sources.

(6) A person who contravenes subsection (2) commits an offence.

(7) The Royal Court may –

(a) on the application of the designated person who is the subject of the information, or

(b) on the application of Her Majesty's Procureur,
grant an injunction to prevent a breach of subsection (2).

PART II
PROHIBITIONS IN RELATION TO DESIGNATED PERSONS

Freezing of funds and economic resources.

9. (1) A person ("P") must not deal with funds or economic resources owned, held or controlled by a designated person if P knows, or has reasonable cause to suspect, that P is dealing with such funds or economic resources.

(2) In subsection (1) "**deal with**" means –

(a) in relation to funds –

(i) use, alter, move, allow access to, or transfer, the funds,

(ii) deal with the funds in any other way that would result in any change in their volume, amount, location, ownership, possession, character or destination, or

(iii) make any other change that would enable use of the funds, including by way of, or in the course of, portfolio management, or

(b) in relation to economic resources, exchange, or use in exchange, for funds, goods or services.

(3) A person who contravenes subsection (1) commits an offence.

Making funds or financial services available to designated person.

10. (1) A person ("P") must not make funds or financial services available (directly or indirectly) to a designated person if P knows, or has reasonable cause to suspect, that P is making the funds or financial services so available.

(2) A person who contravenes subsection (1) commits an offence.

Making funds or financial services available for benefit of designated person.

11. (1) A person ("P") must not make funds or financial services available to any person for the benefit of a designated person if P knows, or has reasonable cause to suspect, that P is making the funds or financial services so available.

(2) For the purposes of subsection (1) –

(a) funds are made available for the benefit of a designated person only if that person thereby obtains, or is able to obtain, a significant financial benefit, and

(b) "**financial benefit**" includes the discharge of a financial obligation for which the designated person is wholly or partly responsible.

(3) A person who contravenes subsection (1) commits an offence.

Making economic resources available to designated person.

12. (1) A person ("P") must not make economic resources available (directly or indirectly) to a designated person if P knows, or has reasonable cause to suspect -

(a) that P is making the economic resources so available, and

(b) that the designated person would be likely to exchange the economic resources, or use them in exchange, for funds, goods or services.

(2) A person who contravenes subsection (1) commits an offence.

Making economic resources available for benefit of designated person.

13. (1) A person ("P") must not make economic resources available to any person for the benefit of a designated person if P knows, or has reasonable cause to suspect, that P is making the economic resources so available.

(2) For the purposes of subsection (1) –

(a) economic resources are made available for the benefit of a designated person only if that person thereby obtains, or is able to obtain, a significant financial benefit, and

(b) "**financial benefit**" includes the discharge of a financial obligation for which the designated person is wholly or partly responsible.

(3) A person who contravenes subsection (1) commits an offence.

Exceptions.

14. (1) The prohibitions in sections 9 to 11 are not contravened by a relevant institution crediting a frozen account with –

(a) interest or other earnings due on the account, or

(b) payments due under contracts, agreements or obligations that were concluded or arose before the account became a frozen account.

(2) The prohibitions in sections 10 and 11 do not prevent a relevant institution from crediting a frozen account where it receives funds transferred to the account.

(3) The prohibition in section 11 is not contravened by the making of a payment that –

(a) is a benefit under or by virtue of a relevant enactment (irrespective of the name or nature of the benefit), and

(b) is made to a person who is not a designated person,
whether or not the payment is made in respect of a designated person.

(4) A relevant institution must without delay inform the Policy Council if it credits a frozen account with a payment referred to in subsection (1)(b) or in the circumstances referred to in subsection (2).

(5) In this section –

"**frozen account**" means an account with a relevant institution which is held or controlled (directly or indirectly) by a designated person, and

"**relevant enactment**" includes the Social Insurance (Guernsey) Law, 1978[i], the Health Service (Benefit) (Guernsey) Law, 1990[j], the Long-term Care Insurance (Guernsey) Law, 2002[k] and such other enactment as the States may by Ordinance prescribe.

Licences.

15. (1) The prohibitions in sections 9 to 13 do not apply to anything done under the authority of a licence granted by the Policy Council under this section.

(2) The Policy Council may grant a licence in respect of a designated person.

(3) A licence granted under this section –

(a) must specify the acts authorized by it,

(b) may be general or granted to a category of persons or to a particular person,

(c) may be unconditional or subject to conditions, and

(d) may be unlimited or limited in duration.

(4) The Policy Council may at any time vary or revoke a licence granted under this section.

(5) On the grant, variation or revocation of a licence under this section, the Policy Council must –

(a) in the case of a licence granted to a particular person, give written notice of the grant, variation or revocation to that person, or

(b) in the case of a general licence or a licence granted to a category of persons, take such steps as the Policy Council considers appropriate to publicize the grant, variation or revocation of the licence.

(6) A person who, for the purpose of obtaining a licence under this section, knowingly or recklessly –

---

i Ordres en Conseil Vol. XXVI, p. 292; Vol. XXVII, pp. 238, 307 and 392; Vol. XXIX, pp. 24, 148 and 422; Vol. XXXII, p. 59; Vol. XXIV, p. 510; Vol. XXXV(1), p. 164; Vol. XXXVI, pp. 123 and 343; Vol. XXXIX, p. 107; Vol. XL, p. 351; Order in Council No. IX of 2001; No. XXIII of 2002; No. XXIV of 2003; No. XI of 2004 and No. XVIII of 2007; Recueil d'Ordonnances Tome XXVI, p. 177 and Ordinance No. XLII of 2009.

j Ordres en Conseil Vol. XXXII, p. 192; Recueil d'Ordonnances Tome XXVI, pp. 177, 483, and 495; Tome XXIX, pp. 182 and 305 and modified by Tome XXVI, pp. 484 and 491; Tome XXVII, p. 200; Tome XXVIII, p. 1; Tome XXIX, pp. 182, 196, 200, 210, 373 and 580; Tome XXXI, p. 628; Tome XXXII, p. 628.

k Order in Council No. XXIII of 2002.

(a) provides information that is false in a material respect, or

(b) provides or produces a document that is not what it purports to be, commits an offence.

(7) A person who purports to act under the authority of a licence granted under this section but fails to comply with any condition to which the licence is subject commits an offence.

Circumventing prohibitions etc.

16. (1) A person must not intentionally participate in activities knowing that the object or effect of them is (whether directly or indirectly) –

(a) to circumvent section 9(1), 10(1), 11(1), 12(1) or 13(1), or

(b) to enable or facilitate the contravention of any of those provisions.

(2) A person who contravenes subsection (1) commits an offence.

PART III
INFORMATION

Reporting obligations of relevant institutions.

17. (1) A relevant institution must inform the Policy Council as soon as practicable if –

(a) it knows, or has reasonable cause to suspect, that a person –

(i) is a designated person, or

(ii) has committed an offence under any provision of Part II, and

(b) the information or other matter on which the knowledge or reasonable cause for suspicion is based came to it in the course of carrying on its business.

(2) Where a relevant institution informs the Policy Council under subsection (1) it must state –

(a) the information or other matter on which the institution's knowledge or reasonable cause for suspicion is based, and

(b) any information that the institution holds about the person by which the person can be identified.

(3) Subsection (4) applies if –

(a) a relevant institution informs the Policy Council under subsection (1) that it knows, or has reasonable cause to suspect, that a person is a designated person, and

(b) that person is a customer of the institution.

(4) The relevant institution must also state the nature and amount or quantity of any funds or economic resources held by it for the customer at the time when it first had the knowledge or suspicion.

(5) A relevant institution that fails to comply with subsection (1) commits an offence.

Powers to require information.

18. (1) The Policy Council may require a designated person to provide information concerning –

(a) funds or economic resources owned, held or controlled by, or on behalf of, the designated person, or

(b) any disposal of such funds or economic resources.

(2) The Policy Council may require a designated person to provide such information as the Policy Council may reasonably require about expenditure –

(a) by or on behalf of the designated person, or

(b) for the benefit of the designated person.

(3) The power in subsection (1) or (2) is exercisable only where the Policy Council believes that it is necessary for the purpose of monitoring compliance with or detecting evasion of this Law.

(4) The Policy Council may require a person acting under a licence granted under section 15 to provide information concerning –

(a) funds or economic resources dealt with under the licence, or

(b) funds, economic resources or financial services made available under the licence.

(5) The Policy Council may require any person in or resident in the Bailiwick to provide such information as the Policy Council may reasonably require for the purpose of –

(a) establishing for the purposes of this Law –

(i) the nature and amount or quantity of any funds or economic resources owned, held or controlled by or on behalf of a designated person,

(ii) the nature and amount or quantity of any funds, economic resources or financial services made available directly or indirectly to, or for the benefit of, a designated person, or

(iii) the nature of any financial transactions entered into by a designated person,

(b) monitoring compliance with or detecting evasion of this Law, or

(c) obtaining evidence of the commission of an offence under this Law.

(6) The Policy Council may specify the manner in which, and the period within which, information is to be provided, being information that the Policy Council requires to be provided under this section.

(7) If no such period is specified, the information so required to be provided must be provided within a reasonable time.

(8) A requirement under this section may impose a continuing obligation to keep the Policy Council informed –

(a) as circumstances change, or

(b) on such regular basis as the Policy Council may specify.

(9) Information required to be provided under this section may relate to any period during which a person is, or was, a designated person.

(10) Information referred to in subsection (1)(b), (2) or (5)(a)(iii) may relate to any period before the person became a designated person (as well as, or instead of, any period of time).

Production of documents.

19. (1) A requirement under section 18 may include a requirement to produce specified documents or documents of a specified description.

(2) Where the Policy Council requires under section 18 that one or more documents be produced, the Policy Council may –

(a) take copies of or extracts from any document so produced,

(b) require any person so producing a document to give an explanation of the document, and

(c) where a person so producing a document is a partnership, association or body corporate, require a person who is –

(i) in the case of a partnership, a present or past partner or employee of the partnership,

(ii) in any other case, a present or past officer or employee of the association or body corporate, to give an explanation of the document.

(3) Where the Policy Council requires under section 18 a designated person, or a person acting under a licence granted under section 15, to produce one or more documents, the person must –

(a) take reasonable steps to obtain the documents (if not already in the person's possession or control), and

(b) keep the documents under the person's possession or control (except for the purpose of providing them to the Policy Council or as the Policy Council may otherwise permit).

Failure to comply with requirement for information.

20. (1) A person commits an offence who –

(a) without reasonable excuse refuses or fails within the time and in the manner specified (or, if no time has been specified, within a reasonable time) to comply with a requirement made under this Part,

(b) knowingly or recklessly gives any information, or produces any document, that is false in a material particular in response to such a requirement,

(c) with intent to evade the provisions of this Part, destroys, mutilates, defaces, conceals or removes a document, or

(d) otherwise intentionally obstructs the Policy Council in the exercise of the Policy Council's powers under this Part.

(2) Where a person is convicted of an offence under this section, the court may make an order requiring the person, within such period as may be specified in the order, to comply with the relevant requirement in accordance with the order, or to do such other thing relating to the requirement as the court orders.

General power to disclose information

21. (1) The Policy Council may disclose any information obtained by it in exercise of its powers under this Part (including any document so obtained and any copy or extract made of any document so obtained) –

(a) to Her Majesty's Procureur,

(b) to a police officer,

(c) to a person holding or acting in any office under or in the service of –

(i) the Crown in right of Her Majesty's Government of the United Kingdom,

(ii) the Crown in right of the Scottish Administration, the Northern Ireland Administration or the Welsh Assembly Government,

(iii) the States, the States of Alderney or the Chief Pleas of Sark,

(iv) the States of Jersey

(v) the Government of the Isle of Man, or

(vi) the Government of any British overseas territory,

(d) to any law officer of the Crown for Jersey or the Isle of Man,

(e) to the Office of the Legal Aid Administrator, the Legal Services Commission of the United Kingdom, the Scottish Legal Aid Board and the Northern Ireland Legal Services Commission,

(f) to the Guernsey Financial Services Commission established by the Financial Services Commission (Bailiwick of Guernsey) Law, 1987[1], the Financial Services Authority of the United Kingdom, the Jersey Financial Services Commission, the Isle of Man Insurance and Pensions Authority and the Isle of Man Financial Supervision Commission,

(g) for the purpose of giving assistance or co-operation, pursuant to the relevant Security Council resolutions, to –

(i) any organ of the United Nations, or

(ii) any person in the service of the United Nations, the Council of the European Union, the European Commission or the Government of any country or territory,

[1] Ordres en Conseil Vol. XXX, p. 243.

(h) with a view to instituting, or otherwise for the purposes of, any proceedings –

(i) in the Bailiwick, for an offence under this Law,

(ii) in the United Kingdom, for an offence under the Terrorist Asset-Freezing etc. Act 2010, or

(iii) in Jersey, in the Isle of Man or in any British overseas territory, for an offence under a similar provision in any such jurisdiction, or

(j) with the consent of a person who, in his or her own right, is entitled to the information or to possession of the document, copy or extract, to a third party.

(2) In subsection (1)(j) "**in his or her own right**" means not merely in the capacity as a servant or agent of another person.

Co-operation with investigations.

22. (1) Her Majesty's Procureur must take such steps as he considers appropriate to co-operate with an investigation relating to the funds, economic resources or financial transactions of a designated person.

(2) The Policy Council must take such steps as it considers appropriate to co-operate with an investigation relating to the funds, economic resources or financial transactions of a designated person.

(3) Subsections (1) and (2) apply whether the investigation takes place in the Bailiwick or elsewhere.

Application of provisions.

23. (1) Nothing done in accordance with this Part is to be treated as a breach of any restriction imposed by contract, enactment or otherwise.

(2) However, nothing in this Part authorizes a disclosure that –

(a) contravenes the Data Protection (Bailiwick of Guernsey) Law, 2001[m], or

(b) is prohibited by Part I of the Regulation of Investigatory Powers (Bailiwick of Guernsey) Law, 2003[n].

---

[m] Order in Council No. V of 2002 as modified by Ordinance No. XXIV of 2004 and No. 2 of 2010; the European Communities (Implementation of Council Directive on Privacy and Electronic Communications) (Sark) Ordinance, 2004 and G.S.I. Nos.14, 15, 16 and 24 of 2002.

[n] Order in Council No. XXX of 2003; as amended by the Machinery of Government (Transfer of Functions) (Guernsey) Ordinance, 2003 (No. XXXIII of 2003); the Regulation of Investigatory Powers (Applicable

(3) Nothing in this Part is to be read as requiring a person ("P") who has acted for another person in the capacity of advocate, counsel or solicitor, or otherwise in the capacity of lawyer, to disclose any privileged information that is in P's possession in that capacity.

(4) This Part does not limit the circumstances in which information may be disclosed otherwise than by virtue of this Part.

(5) This Part does not limit the powers of the Policy Council to impose conditions in connection with the performance of the Policy Council's functions under section 15.

(6) In this section –

"**information**" includes documents, and

"**privileged information**" means information with respect to which a claim to legal professional privilege could be maintained in legal proceedings.

PART IV
SUPPLEMENTARY PROVISIONS

Appeals.

24. (1) This section applies to any decision of the Policy Council taken in the performance of, or in connection with, its functions under this Law including, for the avoidance of doubt, any decision –

(a) to make or vary an interim or final designation of a person,

(b) to renew a final designation of a person, or

(c) not to vary or revoke an interim or final designation of a person.

(2) A person aggrieved by a decision to which this section applies may appeal to the Royal Court against that decision on the grounds that –

(a) the decision was ultra vires or there was some other error of law,

(b) the decision was unreasonable,

(c) the decision was made in bad faith,

(d) there was a lack of proportionality, or

(e) there was a material error as to the facts or as to the procedure.

(3) An appeal under this section shall be instituted –

(a) within 28 days of the date on which notice in writing of the decision was served by the Policy Council on the person to whom the decision relates, or such later date as the Royal Court may for good cause allow, and

(b) by a summons served on the Policy Council stating the grounds, and setting out the material facts, on which the appellant relies.

(4) If an appeal under this section has not been determined by the Royal Court within three months of the date of the summons by which it was instituted, the Policy Council may apply to the Royal Court, by a summons served on the appellant, to show cause why the appeal should not be dismissed for want of prosecution; and upon the making of such an application the Royal Court may dismiss the appeal or make such other order as it considers just.

(5) On an appeal under this section the Court may –

(a) set the decision of the Policy Council aside and, if the Court considers it appropriate to do so, remit the matter to the Policy Council with such directions as the Court thinks fit, or

(b) confirm the decision, in whole or in part.

(6) A decision of the Royal Court under this section shall be final as to any question of fact, but an appeal from such a decision shall lie to the Court of Appeal on any question of law within such period and in such manner as may be prescribed by Order of the Royal Court.

(7) The making of an appeal under this section does not suspend the effect of the decision to which the appeal relates.

Special Court Procedures.

25. (1) The States may by Ordinance provide for special court procedures to be followed in any proceedings –

(a) under this Law,

(b) under any other enactment concerning the freezing of assets, or

(c) under other measures giving effect to international sanctions.

(2) An Ordinance under subsection (1) may, without limitation, make provision in relation to the following matters –

(a) the mode of proof and evidence in the proceedings,

(b) the disclosure of evidence and any other matter relating to the proceedings,

(c) the determination of the proceedings, or any issue in the proceedings, including determination –

(i) without a hearing,

(ii) without the provision to any party to the proceedings (or to the legal representative of any such party) of full particulars of the reasons for any decision relating to the proceedings or issue, and

(iii) in the absence of any person, including any party to the proceedings (or the legal representative of any such party),

(d) legal representation in the proceedings,

(e) rights of audience in the proceedings,

(f) the establishment of a tribunal or other body with powers to determine the proceedings, and

(g) the authorisation of, and conferring of functions on, any court, tribunal or other body in order to enable any such court, tribunal or body to determine the proceedings or any issue in the proceedings.

(3) The Royal Court must be consulted in connection with any Ordinance made under this section.

PART V
OFFENCES

Penalties.

26. (1) A person guilty of an offence under section 9(3), 10(2), 11(3), 12(2), 13(3), or 16(2) is liable –

(a) an conviction on indictment, to imprisonment for a term not exceeding seven years or to a fine or to both, or

(b) on summary conviction, to imprisonment for a term not exceeding 12 months or to a fine not exceeding level 4 on the uniform scale or to both.

(2) A person guilty of an offence under section 8(6) or 15(6) or (7) is liable –

(a) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both, or

(b) on summary conviction, to imprisonment for a term not exceeding 12 months or to a fine not exceeding level 4 on the uniform scale or to both.

(3) A person guilty of an offence under section 17(5) or 20(1) is liable on summary conviction to imprisonment for a term not exceeding 12 months or to a fine not exceeding level 4 on the uniform scale or to both.

Extra-territorial application of offences.

27. (1) An offence under this Law may be committed by conduct wholly or partly outside the Bailiwick by –

(a) a UK national who is ordinarily resident in the Bailiwick, or

(b) a body incorporated or constituted under the law of the Bailiwick or any part thereof.

(2) In subsection (1) "**UK national**" means –

(a) a British citizen, a British overseas territories citizen, a British National (Overseas) or a British Overseas citizen all within the meaning of the British Nationality Act 1981[o],

(b) a person who under that Act is a British subject, or

(c) a British protected person within the meaning of that Act.

(3) In this section "**conduct**" includes acts and omissions.

(4) Nothing in this section affects any criminal liability arising otherwise than under this section.

Offences by bodies corporate, etc.

28. (1) Where an offence under this Law is committed by a body corporate or by an unincorporated body and is proved to have been committed with the consent or connivance of, or to be attributable to or to have been facilitated by any neglect on the part of, any director, manager, member of any committee of management or other controlling authority, secretary or other similar officer or partner of the body, or any person purporting to act in any such capacity, he as well as the body is guilty of the offence and may be proceeded against and punished accordingly.

---

[o] An Act of Parliament (1981 c.61).

(2) Where the affairs of a body corporate are managed by its members, subsection (1) applies to a member in connection with his functions of management as if he were a director.

(3) Proceedings for an offence alleged to have been committed under this Law by an unincorporated body shall be brought in the name of that body and not in the name of any of its members, and a fine imposed on the body on its conviction of such an offence shall be paid out of its funds.

(4) For the purposes of this section a person shall be deemed to be a director of a body corporate if he is a person in accordance with whose directions or instructions the directors of the body corporate or any of them act.

Jurisdiction to try offences.

29. Where an offence under this Part is committed outside the Bailiwick-

(a) proceedings for the offence may be taken in Guernsey, and

(b) the offence may for all incidental purposes be treated as having been committed in Guernsey.

PART VI
INTERPRETATION

Meaning of "funds" and "economic resources".

30. (1) In this Law, "**funds**" means financial assets and benefits of every kind, including, without limitation –

(a) cash, cheques, claims on money, drafts, money orders and other payment instruments,

(b) deposits with relevant institutions or other persons, balances on accounts, debts and debt obligations,

(c) publicly and privately traded securities and debt instruments, including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures and derivative products,

(d) interest, dividends and other income on or value accruing from or generated by assets,

(e) credit, rights of set-off, guarantees, performance bonds and other financial commitments,

(f) letters of credit, bills of lading and bills of sale,

(g) documents providing evidence of an interest in funds or financial resources,

(h) any other instrument of export financing.

(2) In this Law, "**economic resources**" means assets of every kind, whether tangible or intangible, movable or immovable, which are not funds but can be used to obtain funds, goods or services.

Meaning of "financial services".

31. (1) In this Law, "**financial services**" means any service of a financial nature, including (but not limited to) –

(a) insurance-related services consisting of –

(i) direct life assurance,

(ii) direct insurance other than life assurance,

(iii) reinsurance and retrocession,

(iv) insurance intermediation, such as brokerage and agency,

(v) services auxiliary to insurance, such as consultancy, actuarial, risk assessment and claim settlement services,

(b) banking and other financial services consisting of –

(i) accepting deposits and other repayable funds,

(ii) lending (including consumer credit, mortgage credit, factoring and financing of commercial transactions),

(iii) financial leasing,

(iv) payment and money transmission services (including credit, charge and debit cards, travellers' cheques and bankers' drafts),

(v) providing guarantees or commitments,

(vi) financial trading (as defined in subsection (2)),

(vii) participating in issues of any kind of securities (including underwriting and placement as an agent, whether publicly or privately) and providing services related to such issues,

(viii) money brokering,

(ix) asset management, such as cash or portfolio management, all forms of collective investment management, pension fund management, custodial, depository and trust services,

(x) settlement and clearing services for financial assets (including securities, derivative products and other negotiable instruments),

(xi) providing or transferring financial information, and financial data processing or related software (but only by suppliers of other financial services),

(xii) providing advisory and other auxiliary financial services in respect of any activity listed in sub-paragraphs (i) to (xi) (including credit reference and analysis, investment and portfolio research and advice, advice on acquisitions and on corporate restructuring and strategy),

(c) any finance business within the meaning of section 24 of the Financial Services Commission (Bailiwick of Guernsey) Law 1987 and not included in subsection (1)(a) and (b).

(2) In subsection (1)(b)(vi), "**financial trading**" means trading for own account or for account of customers, whether on an investment exchange, in an over-the-counter market or otherwise, in –

(a) money market instruments (including cheques, bills and certificates of deposit),

(b) foreign exchange,

(c) derivative products (including futures and options),

(d) exchange rate and interest rate instruments (including products such as swaps and forward rate agreements),

(e) transferable securities, or

(f) other negotiable instruments and financial assets (including bullion).

Meaning of "relevant institution".

32. (1) In this Law, "**relevant institution**" means –

(a) a person (whether or not an individual) that carries on financial services business in or from the Bailiwick, or

(b) a person (not being an individual) who is incorporated or constituted under the law of the Bailiwick or any part thereof and carries on financial services business in any part of the world.

(2) For the purposes of subsection (1), "**financial services business**" has the same meaning as in the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999[p].

Interpretation: general.

33. (1) In this Law, unless the context otherwise requires –

"**advocate**" means an Advocate of the Royal Court of Guernsey,

"**Bailiff**" includes the Deputy Bailiff, a Lieutenant Bailiff and any Judge of the Royal Court,

"**Bailiwick**" means the Bailiwick of Guernsey,

"**British overseas territory**" has the same meaning as in the British Nationality Act 1981,

"**community provision**" has the meaning given by section 3(1) of the the European Communities (Implementation) (Bailiwick of Guernsey) Law, 1994[q],

"**Court of Appeal**" means the court established by the Court of Appeal (Guernsey) Law, 1961[r],

"customs officer" means an officer within the meaning of section 1(1) of the Customs and Excise (General Provisions) (Bailiwick of Guernsey) Law, 1972[s],

"**designated person**" has the meaning given by section 1,

"**document**" includes information recorded in any form and, in relation to information recorded otherwise than in legible form, references to its production include producing a copy of the information in legible form,

"**enactment**" means any Law, Ordinance or subordinate legislation,

---

p Ordres en Conseil Vol. XXXIX, p. 137; amended by Order in Council No. II of 2005; No. XV of 2007 and No. XIII of 2010; Recueil d'Ordonnances Tome XXVIII, pp. 266 and 274; Tome XXIX, pp. 112 and 406 and Tome XXXII, p. 666; Ordinance No. XXXVII of 2008 and Nos. XVI and XXXIV of 2010; G.S.I. No. 27 of 2002; No. 43 of 2006; No. 33 of 2007; Nos. 48 and 73 of 2008 and No. 12 of 2010.

q Ordres en Conseil Vol. XXXV(1), p. 65.

r Ordres en Conseil Vol. XVIII, p.315.

s Ordres en Conseil Vol. XXIII, p. 573; Vol. XXIV, p. 87; Vol. XXXI, p. 278 and Vol. XXXIII, p. 217; Order in Council No. X of 2004.

"**economic resources**" has the meaning given by section 30(2),

"**final designation"** means a designation under section 4 (including any renewed such designation),

"**financial services**" has the meaning given by section 31,

"**funds**" has the meaning given by section 30(1),

"**Her Majesty's Procureur**" includes Her Majesty's Comptroller,

"**interim designation**" means a designation under section 2,

"**international sanctions**" include sanctions adopted by the Security Council of the United Nations and sanctions under any community provision,

"**Jersey**" means the Bailiwick of Jersey,

"**the Office of the Legal Aid Administrator**" means the office established under section 2(1) of the Legal Aid (Bailiwick of Guernsey) Law, 2003[t],

"**police officer**" means –

(a) a member of the salaried police force of the Island of Guernsey, and

(b) within the limits of his jurisdiction, a member of the special constabulary of the Island of Guernsey, and includes a customs officer,

"**relevant institution"** has the meaning given by section 32,

"**relevant Security Council resolutions**" means –

(a) resolution 1373 (2001) adopted by the Security Council of the United Nations on 28th September 2001,

(b) resolution 1452 (2002) adopted by the Security Council of the United Nations on 20th December 2002, and

(c) such other resolution as the Policy Council may by order prescribe,

"**renew**" means, in respect of a final designation, renew under section 5,

"**the Royal Court**" means the Royal Court of Guernsey sitting as an Ordinary Court and for the purposes of this Law the Royal Court is constituted by the Bailiff sitting unaccompanied by the Jurats,

---

[t] Order in Council No. VI of 2004 and see Recueil d'Ordonnaces Tome XXIX, p. 406.

"**the States**" means the States of Guernsey,

"**subordinate legislation**" means any regulation, rule, order, notice, rule of court, resolution, scheme, warrant, byelaw or other instrument made under any enactment and having legislative effect,

"**terrorism**" has the same meaning as in the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002[u], and

"**uniform scale**" means the uniform scale of fines for the time being in force under the Uniform Scale of Fines (Bailiwick of Guernsey) Law, 1989[v].

(2) The provisions of the Interpretation (Guernsey) Law, 1948[w] shall apply to the interpretation of this Law throughout the Bailiwick.

(3) A reference in this Law to any enactment, to the relevant Security Council resolutions and any Act of Parliament is a reference to that enactment, those resolutions and that Act as amended from time to time.

PART VII
MISCELLANEOUS

Service of notices.

34. (1) This section applies in relation to any notice to be given to a person by the Policy Council under this Law.

(2) Any such notice may be given –

(a) by posting it to the person's last known address, or

(b) where the person is a body corporate, partnership or unincorporated body other than a partnership, by posting it to the registered or principal office of the body or partnership concerned.

(3) Where the Policy Council does not have an address for the person, it must make arrangements for the notice to be given to the person at the first available opportunity.

Delegation.

35. (1) The Policy Council may, by instrument in writing, delegate wholly or partly any of its functions under this Law to any other person or to any body.

---

[u] Order in Council No. XVI of 2002.

[v] Ordres en Conseil Vol. XXXI, p. 278; Recueil d'Ordonnances Tome XXV, p. 344; Tome XXVIII, p. 89 and Tome XXXI, p. 542.

[w] Ordres en Conseil Vol. XIII, p. 355.

(2) The delegation may be unconditional or subject to any condition specified in the instrument of delegation.

(3) The delegation of functions by the Policy Council under this section shall not prevent the Policy Council from itself performing those functions.

(4) Where any licence, permit or authorization is granted in purported performance of a function delegated under subsection (1), no criminal proceedings shall lie against any person for any act done, or omitted to be done, in good faith and in accordance with the terms of the licence, permit or authorization, by reason that the function had not been delegated, or that any requirement attached to the delegation of the function had not been complied with.

(5) Nothing in this section affects the operation of section 4 of the Public Functions (Transfer and Performance) (Bailiwick of Guernsey) Law 1991[x].

Consequential amendments.

36. The Schedule (amendments consequential on this Law) shall have effect.

Power to give effect by Ordinance.

37. (1) The States may by Ordinance make such additional or alternative provision as they think fit for the purposes of giving effect to the relevant Security Council resolutions throughout the Bailiwick including, without limitation, provision amending this Law.

(2) The provisions of subsection (1) are without prejudice to any other provision of this Law conferring power to enact Ordinances (and vice versa).

General provisions as to Ordinances and orders.

38. (1) An Ordinance or order under this Law –

(a) may be amended or repealed by a subsequent Ordinance or order hereunder, and

(b) in the case of an Ordinance, may contain such consequential, incidental, supplementary, transitional and savings provisions as may appear to be necessary or expedient (including, without limitation, provision making consequential amendments to this Law and any other enactment).

(2) Any power to make an Ordinance or order may be exercised –

[x] Ordres en Conseil Vol. XXXIII, p. 478.

(a) in relation to all cases to which the power extends, or in relation to all those cases subject to specified exceptions, or in relation to any specified cases or classes of cases,

(b) so as to make, as respects the cases in relation to which it is exercised –

(i) the full provision to which the power extends, or any lesser provision (whether by way of exception or otherwise),

(ii) the same provision for all cases, or different provision for different cases or classes of cases, or different provision for the same case or class of case for different purposes, or

(iii) any such provision either unconditionally or subject to any prescribed conditions.

(3) An order (other than rules or an order of a court or tribunal) under this Law shall be laid before a meeting of the States as soon as possible after being made; and, if at that or the next meeting the States resolve that the order be annulled, then the order shall cease to have effect, but without prejudice to anything done under the order or to the making of a new order.

Citation and commencement.

39. (1) This Law may be cited as the Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011.

(2) This Law shall come into operation on the day appointed by Ordinance of the States, and such an Ordinance may appoint different days for different provisions and different purposes.

Section 36

SCHEDULE
AMENDMENTS CONSEQUENTIAL ON THIS LAW

Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999.

1. In the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999

(a) in section 49(6), in the definition of money laundering, immediately after "section 8, 9, 10 or 11 of the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002", insert ", or section 9, 10, 11, 12 or 13 of the Terrorist Asset Freezing (Bailiwick of Guernsey) Law 2011",

(b) in section 49A(6), in the definition of money laundering, immediately after "section 8, 9, 10 or 11 of the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002" insert ", or section 9, 10, 11, 12 or 13 of the Terrorist Asset Freezing (Bailiwick of Guernsey) Law 2011".

Terrorism and Crime (Bailiwick of Guernsey) Law, 2002.

2. In section 79(1) of the Terrorism and Crime (Bailiwick of Guernsey) Law 2002, in the definition of terrorist financing, immediately after "section 8, 9, 10 or 11", insert ", or section 9, 10, 11, 12 or 13 of the Terrorist Asset Freezing (Bailiwick of Guernsey) Law 2011".

Transfer of Funds (Guernsey) Ordinance, 2007.

3. In section 10(1) of the Transfer of Funds (Guernsey) Ordinance, 2007[y] -

(a) in subparagraph (vi), omit "or", and

(b) immediately after subparagraph (vii), insert –

"or

(viii) the Al-Qaida and Taliban (Freezing of Funds) (Guernsey) Ordinance, 2011, or

(ix) the Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011,".

[y] Recueil d'Ordonnances Tome XXXII, p. 194.

Transfer of Funds (Alderney) Ordinance, 2007.

4. In section 10(1) of the Transfer of Funds (Alderney) Ordinance, 2007[z] –

(a) in subparagraph (vi), omit "or", and

(b) immediately after subparagraph (vii), insert –

"or

(viii) the Al-Qaida and Taliban (Freezing of Funds) (Guernsey) Ordinance, 2011, or

(ix) the Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011,".

Transfer of Funds (Sark) Ordinance, 2007.

5. In section 10(1) of the Transfer of Funds (Sark) Ordinance, 2007[aa] -

(a) in subparagraph (vi), omit "or", and

(b) immediately after subparagraph (vii), insert –

"or

(viii) the Al-Qaida and Taliban (Freezing of Funds) (Guernsey) Ordinance, 2011, or

(ix) the Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011,".

Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2007.

6. In regulation 19(1) of the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2007[bb], in subparagraph (a) of the definition of "terrorist financing", immediately after "section 8, 9, 10 or 11 of the Terrorism Law" insert ", or section 9, 10, 11, 12 or 13 of the Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011".

Criminal Justice (Proceeds of Crime) (Legal Professionals, Accountants and Estate Agents) (Bailiwick of Guernsey) Regulations, 2008.

7. In regulation 30(1) of the Criminal Justice (Proceeds of Crime) (Legal Professionals, Accountants and Estate Agents) (Bailiwick of Guernsey)

---

[z] Alderney Ordinances No. VI of 2007.
[aa] Folio No. 157.
[bb] G.S.I. No. 33 of 2007.

Regulations, 2008[cc], in subparagraph (a) of the definition of "terrorist financing", immediately after "section 8, 9, 10 or 11 of the Terrorism Law" insert ", or section 9, 10, 11, 12 or 13 of the Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011".

[cc] G.S.I. No. 49 of 2008.

CHAPTER 17 – GLOSSARY

Sections in this Chapter

17 GLOSSARY

17.1 Glossary of Terms

Account:

Account means a bank account and any other business relationship between a financial services business and a customer which is of a similar nature having regard to the services offered by the financial services business.

Appropriately qualified:

A requirement for a person to be appropriately qualified means that the person must have appropriate knowledge, skill or experience for the relevant position.

Associated account:

Associated account refers to an account with the same financial services business where any of the principals are connected with an account in the same group or structure.

Account activity:

The provision of an estimate of the total flow of funds in and out of an account together with an estimate of the expected maximum account turnover.

Batch transfer:

A batch transfer is a transfer comprised of a number of individual wire transfers that are being sent to the same financial services businesses, but may/may not be ultimately intended for different persons.

Bearer negotiable instruments:

Includes 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:

These are negotiable instruments that accord ownership in a corporation to the person who possesses the bearer share certificate.

Beneficial owner:

The natural person who ultimately owns or controls the customer, and a person on whose behalf the business relationship or occasional transaction is to be or is being conducted and, in the case of a foundation, trust or other legal arrangements, this shall mean any beneficiary in whom an interest has vested, and any other person who benefits from that foundation, trust or other legal arrangement.

Board:

References in the Handbook to the Board refer to the board of directors of a financial services business, where it is a body corporate, or the senior management of a financial services business, where it is not a body corporate.

Business relationship:

A business, professional or commercial relationship between a financial services business and a customer which is expected by the financial services business, at the time when contact is established, to have an element of duration.

Business risk assessment:

An assessment which documents the exposure of a business to money laundering and terrorist financing risks and vulnerabilities taking into account its size, nature and complexity and its customers, products and services and the ways in which it provides those services.

Cross-border transfer:

A cross-border transfer refers to any wire transfer where the originator and beneficiary institutions are located in different countries or territories. This term also refers to any chain of wire transfers that has at least one cross-border element.

Customer:

A person or legal arrangement who is seeking to establish or has established, a business relationship with a financial services business, or to carry out or has carried out, an occasional transaction with a financial services 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:

The steps which a financial services business is required to carry out in order to identify and verify the identity of the parties to a relationship and to obtain information on the purpose and intended nature of each business relationship and occasional transaction.

Customer due diligence information:

Identification data and any account files and correspondence relating to the business relationship or occasional transaction.

Document:

Includes information recorded in any form (including, without limitation, in electronic form).

Domestic transfer:

Any wire transfer where the originator and beneficiary institutions are located in the same country or territory. This term therefore refers to any chain of wire transfers that takes place entirely within the borders of a single country or territory, even though the system used to effect the wire transfer may be located in another country or territory.

Employee:

An individual working, including on a temporary basis, for a financial services business whether under a contract of employment, a contract for services or otherwise.

Express trust:

A trust clearly created by the settlor, usually in the form of a document, for example, a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangement (for example, a constructive trust).

FATF Recommendations:

The International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation issued by the Financial Action Task Force.

Financial exclusion:

Where 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.

FIS:

Police Officers and Customs Officers who are members of the Financial Intelligence Service.

Financial services business:

As defined in the schedule to the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999, as amended by the Criminal Justice (Proceeds of Crime)

(Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2007 as amended and includes, unless the context otherwise requires, a person carrying on such a business.

Foreign counterparts:

Authorities in another country or territory that exercise similar responsibilities and functions to the domestic authority referenced.

Foundation:

(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:

(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 subparagraph (a).

Founder:

(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 subparagraph (a).

Funds:

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.

Funds transfer:

A transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.

Handbook:

The Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing as revised or re-issued from time to time by the Commission.

Identification data:

Data, documents or information, in any form whatsoever, which is from a reliable and independent source.

Intermediary:

A financial services business, or a firm of lawyers or estate agents operating in Guernsey, which is considered as being the customer of a financial services business when establishing a business relationship or undertaking an occasional transaction, in accordance with chapter 6 of the Handbook.

Introducer:

A financial services 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 financial services business.

Legal arrangement:

An express trust or any other vehicle whatsoever which has a similar legal effect.

Legal body:

Bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial services business or otherwise own property.

Maintain:

The regulatory requirements of the Handbook make it clear that maintain in this context is to be read to mean that relevant policies, procedures and controls must be established, implemented and that the financial services business must monitor such policies, procedures and controls to ensure that they are operating effectively.

Occasional transaction:

Any transaction where a business relationship has not been established and the transaction is more than £10,000. This includes situations where the transaction is carried out in a single operation or in several operations that appear to be linked. Transactions separated by an interval of three months or more, are not required, in the absence of evidence to the contrary, to be treated as linked.

Originator/Payer:

The account holder, or where there is no account, the person (natural or legal) that places the order with the financial services business to perform the wire transfer.

PEPs:

Individuals who are or have been entrusted with prominent public functions in a country or territory other than Guernsey, for example. Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Proceeds:

Refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.

Regulated financial services business:

A financial services business which is subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and supervised for compliance with those requirements and which operates from Guernsey or a country or territory listed in Appendix C to the Handbook.

Regulated market:

As defined in section 9 of the Insider Dealing (Securities and Regulated Markets) Order, 1996 as amended.

Relevant employees:

"Relevant employees" means any-

(a) member of the board,
(b) member of the management of the financial services business,
(c) employees whose duties relate to the financial services business, and
(d) other employees who are exposed to the risk of money laundering and terrorist financing.

Relevant person:

Relevant person in the context of a foundation means the registered agent, foundation official or any other person who holds information on the identity of the underlying principals and beneficial owners of the foundation.

Satisfied:

Where reference is made to a financial services business being satisfied as to a matter, that financial services business must be able to justify and demonstrate its assessment to the Commission.

Settlor:

Persons or companies who transfer ownership of their assets to trustees.

Shell bank:

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.

Termination:

The conclusion of the relationship between the financial services 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/client.

Transactions:

In the general context of the Handbook, the reference to transactions should be understood to include occasional transactions, any customer facing functions, or the handling of business relationships.

Transaction document:

A document which is a record of a transaction carried out by a financial services business with a customer or an introducer.

Underlying principal:

In relation to a business relationship or occasional transaction, any person who is not a beneficial owner but who is a settlor, trustee, protector or enforcer of a trust, or a founder or foundation official (including councillors and guardians) of a foundation which is the customer or the beneficiaries of which are the beneficial owners, or exercises ultimate effective control over the customer or exercises or is to exercise such control over the business relationship or occasional transaction.

Unique identifier:

Any unique combination of letters, numbers or symbols that refers to a specific originator.

Vested interest:

An interest which, whether or not currently in possession, is not contingent or conditional on the occurrence of any event.

Wire transfer:

Any transaction carried out on behalf of an originator person (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 originator and the beneficiary may be the same person.

Annex to the Financial Services Businesses Handbook

Using Technology in the Customer Due Diligence Process

A financial services business must comply with the Rules in addition to the Regulations. The Rules are boxed and shaded for ease of reference. A financial services business should note that the Court must take into account the Rules and Guidance issued by the Commission in considering compliance with the Regulations.

A.1. Technology Risk Evaluation

1. A financial services business must, prior to deciding whether to utilise an electronic method or system in its due diligence process, have identified and assessed the risks arising from its use and documented these risks in a technology risk evaluation.

2. If a financial services business decides to proceed with the electronic method or system, the financial services business's Board must approve the technology risk evaluation and that approval must be documented.

3. The Board must regularly review the technology risk evaluation in conjunction with its responsibility for oversight of compliance as described under section 2.3 of the Handbook. The Board must record its confirmation that compliance with the Regulations and rules in the Handbook is maintained by its utilisation of the electronic method or system.

4. The technology risk evaluation applies only to the use of, or potential use of: digital signatures; electronic certification; and electronic verification.

5. Although the Board must undertake regular reviews in accordance with rule 3 to the Annex, the technology risk evaluation need only be updated when significant changes or upgrades to technological systems are implemented.

A.1.1. Technology Risk Evaluation Scope

6. The technology risk evaluation should include, as a minimum, an evaluation of the provider, the electronic method or system and its anticipated use, together with any identified risks associated with these areas.

7. It is not essential that the technology risk evaluation extend to a highly technical comprehensive report on the specifications and functionality. The objective of the technology risk evaluation is to evaluate the risks inherent in the use of an electronic method or system.

8. The use of electronic databases, such as electoral registers and addresses from national telephone records, does not require compilation of or inclusion in a technology risk evaluation. In such cases financial services businesses should monitor performance as part of their oversight of compliance monitoring obligations under rule 28.

A.1.2. Areas to Consider when Evaluating an Electronic Method or System

9. The following points are guidelines and examples of points to consider when undertaking a technology risk evaluation. The guidelines are not exhaustive of every factor for consideration, neither are they proposed as a checklist. The guidelines propose a wide range of factors that could be considered in order to cater for the different types of electronic method or service a financial services business might contemplate using. It is acknowledged that in some instances financial services businesses may elect to use alternative or a limited number of the factors listed due to the type of electronic method or system being introduced.

A.1.2.1. Data

- What are the data sources used and the level of accessibility?
- Where is the data stored?
- What are the levels of user security and accessibility?
- What are the methods used to transfer data and documents?
- Are there adequate controls regarding the security of data?
- Who owns the data and documentation collected? If an outsourced provider retains the data and documentation then is there a contract or contingency plan to recover any data in the event of any changes occurring in the relationship with the provider?
- Is there an ability to select and change the data sources used?
- Does the result of the change maintain compliance with data protection legislation?
- Is it necessary to obtain customer consent in order to obtain, research or retain data?
- What are the security controls surrounding the system?
- What is the testing undertaken by a provider to ensure that their data sources are and continue to be accurate and reliable?

A.1.2.2. Controls

- Does the financial services business's existing fraud prevention policy and procedures need alignment or require amendment to accommodate process changes introduced through the technology?
- Does the financial services business's business continuity plan consider and cater for contingency plans for disruption of the electronic method or system?
- Whether there are mechanisms in place to maintain consistency with current and any future changes in international standards and requirements?

A.1.2.3. External Service or Product Providers

- If an external provider is used, is there knowledge and documentation of the system and transparency of the methodologies used by the provider?
- Is there a capability to cancel any arrangement with an external provider?
- Does the provider have a business continuity plan?

A.1.2.4. Information Sources

- What source(s) of information are used to corroborate any information provided and are they acceptable to the financial services business?
- Is there an independent and reliable source to corroborate any information?
- Are a wide range of qualitative and informative sources accessed to corroborate data?
- Are the data sources able to link an individual to both current and previous circumstances, i.e. can the method or system access negative information sources, such as databases on identity fraud and deceased persons?
- How is information matched and corroborated and is this effective?
- What is the extent of the data held, i.e. how up to date is it?
- Is it possible to obtain the full range of identification data or is there an alternative process to acquire mandatory ID data not included within the identification documents?

A.1.2.5. Processes

- What is the assurance of security and authenticity of the method used to validate a customer's details?
- If photographs are taken of an individual and/or documents, how are they compared and checked to ensure authenticity?
- Is a single photograph taken, a series of photos or a video clip acquired?
- Are biometric comparisons used to validate facial features?
- For e-passports does the system read the biometric and other data stored on the embedded chip within the passport and compare it to the data on the passport and that provided by the individual?
- For systems that obtain an individual's photograph and make a comparison against other documents, does it provide a clear match or a percentage of assurance?
- What detection methods are used to provide for changes in identification photographs?
- What is the quality of the electronic record; are photographs clear, in colour and can all data be viewed or enlarged to add clarity?
- What methods are used to ensure that any documents are not altered or tampered?
- Are the documents subjected to independent scrutiny by personnel skilled in identifying potentially fraudulent documents?
- What testing is undertaken to ensure that the new technology method/system can detect fraudulent customers and documentation?

A.2. Maintaining the Effectiveness of Policies, Procedures & Controls

10. A financial services business must ensure that its AML/CFT policies and procedures contain a description which adequately explains how the electronic method or system operates and interacts with its wider AML/CFT controls.

11. The Handbook requires financial services businesses to ensure that there are appropriate and effective procedures and controls in place which provide for the Board to meet its obligation to review its compliance arrangements. Financial services businesses should ensure that procedures and controls accurately include instances where an electronic method or system has been implemented so as to correctly depict their processes.

12. The obligations to identify and verify an individual or a legal body or legal arrangement remain unchanged regardless of the electronic method or system used for CDD purposes.

A.3. Electronic Certification and Digital Signatures

A.3.1. An Introduction to Digital Signatures

13. Digital signatures are based on Public Key Infrastructure ("PKI") technology and guarantee signer identity and intent, data integrity, and the non-repudiation of signed documents. A digital signature should not be capable of being copied, tampered with or altered. In addition, because digital signatures are based on standard PKI technology, they can be validated by anyone without the need for proprietary verification software.

14. A digital signature is a secure method of cryptographically binding an electronic identity to a specific document. A digital signature is a mathematical technique used to validate the authenticity and integrity of an electronic message or document and creates a unique 'hash' based upon the data contained within the document or message being signed.

15. The use of digital signatures provides financial services businesses with the ability to send and receive documentation in an electronic format negating the requirement for an original ink signature or 'wet signature'.

A.3.2. Digital Signatures vs. Electronic Signatures

16. The term electronic signature is often confused with digital signature. Digital signature refers to the security technology used in e-business and e-commerce applications, including electronic signatures. An electronic signature applied with digital signature security provides added assurance to the receiving party of the provenance, identity and status of an electronic document. Additionally, a digital signature acknowledges informed consent and approval by a signatory and ensures the non-repudiation of documents.

17. An electronic signature is any electronic means that indicates either that a person adopts the content of an electronic message, or more broadly that the person who claims to have written a message is the one who wrote it. An electronic signature can be as basic as a typed name or a digitised handwritten signature applied to a document as an image using a stylus.

18. An electronic signature can further be defined as data in electronic form that is attached to or logically associated with other electronic data and that serves as a method of authentication. An electronic signature is an unsecure method of signing a document and is vulnerable to forgery, copying and tampering. Additionally, an electronic signature does not provide an assurance to the receiving party that the document has not been changed, or that the person signing is who they say they are and that they intended to sign the document.

A.3.3. Key Documents

19. The following legislation are key references in respect of this facility:

- The Electronic Transactions (Guernsey) Law, 2000 as amended.
- The Electronic Signatures Directive 1999/93/EC.
- With effect from 1 July 2016 a new regulatory framework (910/2014/EU) will replace the Directive on Electronic Signature (1999/93/EC).
- EU Regulation 910/2014.

A.3.4. Document Security of Digital Signatures

20. Although a digital signature produces a tamper evident seal, financial services businesses should ensure that their procedures provide for confirmation of the authenticity of a digital signature. The procedures should also include the measures to be taken in the event that checks do not confirm the integrity of a digitally signed document.

A.3.5. Digital Signatures Technology Risk Evaluation

21. Due to the security controls and authentication of the source document, an attached digital signature provides confidence that the received document is genuine and not tampered with in any manner.

22. If a financial services business decides to accept and/or use digital signature technology then they should conduct a technology risk evaluation of the system and its anticipated use. Guidelines for the completion of a technology risk evaluation are included in Section A.1.

23. The technology risk evaluation for the use of digital signatures need only be conducted to the extent that the Board of a financial services business is satisfied that the use of digital signatures continues to maintain compliance with existing policies, procedures and controls.

24. The technology risk evaluation should extend to confirming that the digital signatory ("the sender") has appropriate authorisation controls in place regarding who is allowed to use the facility. The sender should be aware that receipt of documents that have a digital signature attached would be considered as authentic and authorised.

A.4. Electronic Certification of Due Diligence Data which is in Paper Form

25. This section applies specifically to the electronic certification of paper documents and not identification data received through the use of an electronic verification method or system as described in section A.5. below.

26. If a financial services business uses an electronic method or system for certification purposes then the rules stated in section 4.5.2 of the Handbook regarding suitable certifiers apply.

27. A financial services business must not employ an electronic method or system which enables a natural person to self-certify their personal identification documents.

28. Where a financial services business accepts electronic certification it must only do so under a digital signature.

29. Should the certifier accept the documentation presented then using digital encryption software the certifier will apply a digital signature to an electronic copy of the physical document.

30. Financial services businesses should use a risk-based approach when deciding whether the certification is adequate and meets the criteria described in paragraph 102 of the Handbook. Best practice is that the certification will incorporate the following:

- confirmation that the certifier has met the individual in question;
- confirmation that the certifier has seen the original(s) of the document(s) being certified;
- the date the document was certified; and
- adequate details about the identity of the certifier in order that the receiving institution can satisfy itself that the certifier is a suitable person in the circumstances.

31. The objective of electronic certification is to confirm a document is a true copy of an original document and financial services businesses should use a risk-based approach to determine whether they are satisfied this has been achieved and if not further measures should be applied.

A.4.1. Risk Mitigation Measures

32. The use of electronic certification is an acceptable form of validating the legitimacy of identity documentation but the accepting financial services business must be satisfied with the veracity of the certification processes.

A.5. Electronic Verification - Using Technology to Verify Identity

A.5.1. Introduction

33. Electronic verification is the use of an electronic method or system to verify, in whole or in part, the identity of a customer by matching specified personal information against electronically captured physical documentation and/or independent electronic sources.

34. The demand to provide faster servicing is increasing the level of development in the use of technology. Systems currently exist that provide varying degrees of certainty regarding the capture of identification data and verification of that information related to individual customers and connected individuals. These 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 prospective customer using an interactive application on a tablet or mobile phone.

35. Rule 87 stipulates the minimum verification requirements. Electronic verification can be used to verify all or any combination of these mandatory verification requirements. Where an electronic verification system does not provide for compliance with all of these requirements then other alternative methods must be used in conjunction with the electronic verification system.

36. Electronic verification is a record kept in an electronic format that contains authenticated core identity information about an individual. Examples include obtaining a photograph or series of photographs of an individual via an application. Photographs are also collected of the identification document(s) and address verification document(s) of the individual. The photographs of the individual and the identity documents are then reviewed and corroborated.

37. The integrated controls inherent within electronic verification applications can provide an acceptable alternative measure to that of Rule 101 when firms are identifying and verifying non-resident customers. Examples of these controls include the reading of biometric information integrated within the microchip on many modern passports or validating the veracity of an official document with its issuing authority. Ultimately it is for the Board to assess the robustness of the verification controls within the application as part of its technology risk evaluation.

A.5.2. Verification of Identity of a Natural Person Using Electronic Verification

38. The fundamental obligation is to establish that any natural person, customer, beneficial owner, underlying principal, third party or third party associate (if applicable) is who they claim to be. Financial services businesses that verify identity through the use of electronic verification must confirm a person's existence on the basis of appropriate identification data that meets the criteria described in chapter 4, Customer Due Diligence, section 4.4.2 of the Handbook.

39. Electronic verification can help:

- identify if there is a person in existence with the personal details of your prospective or existing customer;

- identify if the address details and history of residency are consistent with details held on commercial databases;
- identify whether there are any criminal judgments against the individual or recorded at the individual's residence;
- identify politically exposed persons or those that are subject to sanctions; and
- mitigate identification fraud through confirmation that the identity relates to a living person.

A.5.3. Verification of Identity of Legal Bodies Using Electronic Verification

40. Electronic verification of the legal status of a legal body can be achieved by accessing online company registry databases or commercial databases that access the legal body's records.

41. It is not sufficient to rely solely upon confirmation of registration with a company registry. A financial services business should ensure that it acquires company details that comply with the stipulated legal body identification and verification criteria described in section 4.6.1.

42. Identification and verification are only two parts of the CDD obligations upon firms. A financial services business should also obtain information on the purpose, intended nature of the relationship, and consider whether the profile is consistent with the financial services business's knowledge of the customer in accordance with the rules in Chapter 3 of the Handbook.

A.5.4. Electronic Verification Risk Mitigation Measures

43. Whilst the use of electronic verification can help to reduce the time and cost involved in gathering information and documentation on a customer, financial services businesses should be mindful of any additional risks posed by placing sole reliance on an electronic method or system. An example is that electronic verification can be impaired due to an inability to verify all of the required identification data.

44. 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 match identification data. The use of more than one confirmation source to match data enhances the assurance of authenticity.

A.5.5. Sources Used to Corroborate Information

45. It is imperative that when a financial services business is determining the means to corroborate information, that the electronic method or system uses sources that are reliable and can sufficiently mitigate exposure to fraud.

46. When considering an electronic method or system financial services businesses should evaluate whether the data collected electronically has been entirely corroborated. For example if an identification document is photographed via an application, what checking occurs to validate the authenticity?

47. If the collected data is checked / compared against external data sources then the technology risk evaluation should include assurance that those external sources are

reliable. For example does the external data provider validate its data from an original source i.e. the identification document issuer?

48. To mitigate the risk of impersonation fraud, financial services businesses could add additional verification through the confirmation of details via a second commercial database or alternatively a further primary verification source. Commercial databases are those usually maintained by an entity that has access to current data collated from a reputable source e.g. address from national telephone records or electoral register. It is for the financial services business to determine choice of a database.

A.6. Record Keeping Requirements

49. The record keeping requirements detailed in chapter 12 of the Handbook remain unchanged. The use of technology to collect and/or store data and documents does not alter the obligations and requirements described in the Handbooks.

50. Financial services businesses should cover in their use of technology risk evaluation the retention of documents in electronic format to ensure they do not incur legal evidential difficulties, for example in civil court proceedings. Retention may be:

- by way of original documents;
- on microfiche;
- in a scanned form;
- in a computer or electronic form.

Annex II
Wire Transfers

Contents of this Chapter

1. Introduction

(1) The Transfer of Funds (Guernsey) Ordinance 2017, along with the parallel ordinances for Alderney and Sark, were brought into force on 26 June 2017 following the EU's enactment of Regulation (EU) 2015/847 on information accompanying transfers of funds ("the EU Regulation") on 20 May 2015. References in this chapter to "the Transfer of Funds Ordinance" should be read as referring to the Transfer of Funds (Guernsey, Sark or Alderney) Ordinance 2017 relevant to the island within which the firm is operating.

(2) Article 1 of the Transfer of Funds Ordinance gives the EU Regulation full force and effect in the Bailiwick, subject to certain adaptations, exceptions and modifications as set out in Schedule 1 to the Transfer of Funds Ordinance.

(3) The Bailiwick and the other Crown Dependencies have received a derogation enabling wire transfers between the British Islands to contain the reduced information requirements 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)

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.

3. Outgoing Transfers – Obligations upon the PSP of the Payer

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.

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) There may be occasions when the PSP of the payer does not know the full name of the payee. This may arise when the payer knows only the surname and the initials of the payee's first name(s). In such circumstances it would be acceptable for the PSP of the payer to use initials with the surname subject to consideration by the PSP that the information given by the payer on the identity of the payee is not misleading and that it is reasonable for the payer not to know the full name of the payee. The PSP of the payer should also be mindful that using the initials of the first name(s) of the payee may not be accepted by the PSP of the payee, which could revert with questions on the identity of the payee or reject the transfer. The full surname of the payee should always be obtained by the PSP of the payer.

(8) In the case of a payer that is a company, a transfer must include either the address at which the company's business is conducted or the customer identification number of the company.

(9) Where the payer is a foreign incorporated company administered in the Bailiwick, the address referred to in Rule 14.3.2.(8) would be that of its administrator.

(10) In the case of a payer that is a trust, a transfer must be accompanied by the address of the trustee or the customer identification number of the trust.

(11) Where a trust has multiple co-trustees, the address referred to in Rule 14.3.2.(10) should be that given to open and maintain the account. Where more than one address has been given to open and maintain that account, those addresses should be used.

(12) 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.

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.

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.

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).

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).

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.

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.

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.

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.

(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.

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.

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.

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.