DRAFT

HANDBOOK ON COUNTERING FINANCIAL CRIME AND THE FINANCING OF TERRORISM

CONTENTS

PART 1 – REGULATORY REQUIREMENTS AND GUIDANCE NOTES

CHAPTER 1 – INTRODUCTION

Sections in this chapter **Page**

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.

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 Financial Action Task Force on Money Laundering's (FATF's) Forty Recommendations on Money Laundering and the IX Special Recommendations on Terrorist Financing. The Handbook on Countering Financial Crime and the Financing of Terrorism (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. 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

4. 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) (Bailiwick of Guernsey) Regulations, 2007 (the Regulations), section 15(6)(a) of the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002, section 15 of the Disclosure (Bailiwick of Guernsey) Law, 2007 and section 15 of the the Transfer of Funds (Guernsey) Ordinance, 2007; the Transfer of Funds (Alderney) Ordinance, 2007 and the Transfer of Funds (Sark) Ordinance, 2007.

5. 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 and guidance made by the Commission (as contained in the Handbook) in determining whether or not a person has complied with the Regulations. [The Proceeds of Crime Law and the Terrorism and Crime Law will need to be amended so that the Courts will take account of rules]

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

- The Money Laundering (Disclosure of Information) (Guernsey) Law, 1995;
- The Money Laundering (Disclosure of Information) (Alderney) Law, 1998 as amended;
- The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended;
- The Drug Trafficking (Bailiwick of Guernsey) Law, 2000 as amended;
- The Money Laundering (Disclosure of Information) (Sark) Law, 2001 as amended;
- The Terrorism (United Nations Measures) (Channel Islands) Order 2001;
- The Al-Qa'ida and Taliban (United Nations Measures) (Channel Islands) Order 2002;
- The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 as amended;
- The Transfer of Funds (Guernsey) Ordinance, 2007;
- The Transfer of Funds (Alderney) Ordinance, 2007;
- The Transfer of Funds (Sark) Ordinance, 2007; and
- The Disclosure (Bailiwick of Guernsey) Law, 2007.

7. 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.

8. For any financial services business 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.

9. 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, and related rules in the Handbook and some of the relevant enactments.

10. 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

11. The Handbook is divided into two 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 I. It also includes appendices and a glossary of terms.

12. The full text of the Regulations is set out in Appendix A. 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.

13. 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. [Under a proposed Bailiwick-wide law, referred to in the consultation paper, the Commission will be able to take enforcement action for contraventions of the Commission Rules by financial services businesses which are not licensed or authorised by the Commission but which are registered with the Commission. It should be noted that, as with licensed or authorised financial services businesses, compliance with the Commission Rules must be taken into account by the courts when considering compliance with the Regulations.]
- Level two (**Guidance**) presents ways of complying with the Regulations and the Commission Rules. A financial services business may adopt other

effective and appropriate 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.

14. 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.

15. 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.

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

17. 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.

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

19. The Handbook is not intended to provide an exhaustive list of effective and appropriate 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 and 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

20. 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 and of the product/service/delivery channel to identify the money laundering and terrorist financing risk to the financial services business;
- risk mitigation – applying effective and appropriate 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.

21. 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.

22. 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 be materially different. An approach to preventing money laundering and terrorist financing that is appropriate in one sector may be inappropriate in another.

23. A financial services business needs to 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. 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) 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,

to the extent that the law of that country or territory allows and if the law of

any country or territory does not so allow in relation to any requirement of the 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 provided in the Handbook in considering compliance with the Regulations.

2.1 Objectives

24. 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

25. 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

26. The Board has effective responsibility for compliance with the Regulations and the Handbook. In particular the Board must take responsibility for the policy on review of compliance and discuss a review of compliance at appropriate intervals.

27. In meeting the requirements of the Regulations, the Board of a financial services business must evaluate and record the evaluation of its compliance with the Commission's document "Guidance on Corporate Governance in the Finance Sector in Guernsey" – see Appendix B.

28. A financial services business must also ensure that there are effective and appropriate 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 appropriateness of the policies, procedures and controls;
- 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; 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 Financial services business conducted outside Guernsey

30. 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.

31. A financial services business must be aware that this situation is particularly likely to occur in countries or territories which do not or insufficiently apply the FATF Recommendations.

2.3.2 Outsourcing

32. 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.

33. 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, where necessary monitor the perceived risk, and ensure that relevant policies, procedures and controls are and continue to be in place at the outsourced business.

34. 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; and
- 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

35. 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.

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

- 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 customer identification and verification records;
- be available on a day to day basis (in his absence the role must be performed by a designated deputy MLRO whose name must be communicated to the employees);
- 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.

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 a suitable and sufficient business risk assessment-

(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;

(b) regularly review its business risk assessment 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;

(c) 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;

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

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

(2) A financial services business must have regard to any relevant rules and guidance in the Handbook 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 provided in the Handbook in considering compliance with the Regulations.

3.1 Objectives

37. 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.

38. 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.

3.2 Benefits of a Risk-Based Approach

39. 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.

40. 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 rather than carrying out a "tick box" approach.

41. 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 effective and appropriate 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

42. 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.

43. 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 geographical origin;
  - the complexity of their legal and transaction structures;
  - the way they were introduced to the financial services business; and
  - the unwillingness of non-personal customers 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

44. In order to ensure its policies, procedures and controls on anti-money laundering and terrorist financing are effective and appropriate, 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.

45. These measures may include:

- varying the identification and verification 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 e.g. identifying and understanding where a customer's funds and wealth come from;
- monitoring ongoing CDD, existing customer accounts and ongoing business relationships.

46. 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

47. The undertaking of a risk assessment of the proposed business relationship or occasional transaction will allow a financial services business to consider the extent of its potential exposure to the risk of money laundering and terrorist financing. 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.

48. A financial services business must have documented procedures which will allow it to demonstrate how the assessment of each business relationship has been reached, taking into account the nature and complexity of its operation. A simple approach, building on the risk that the customer base and the range of products and services offered are assessed to present, may be appropriate in some circumstances provided that the financial services business has satisfied itself, on reasonable grounds, that such an approach effectively assesses the risk for the particular business relationship or occasional transaction.

49. A financial services business with a diverse customer base or where a wide range of products and services are available must develop a more complex system to show that judgement has been exercised on an individual basis rather than on a generic or

categorised basis.

50. Consideration of the information obtained from the process of assessment will assist a financial services business in establishing a risk profile for each business relationship – see section 3.8.

51. The process of assessment may identify risks which a financial services business does not consider can satisfactorily be managed or mitigated and, in such cases, it should consider whether it is appropriate to enter into or continue the business relationship.

52. The general policy of each financial services business towards the identification and assessment of risk in its customer base should be documented and approved at Board level.

3.6 Monitoring the Effectiveness of Policies, Procedures and Controls

53. The financial services business' compliance review policy must make provision for a review of the following elements and its board discussion on compliance review must include a review of the same:

- the procedures surrounding the products/services offered by the financial services business;
- the identification and verification requirements in place for establishing a new business relationship;
- staff screening and training; and
- monitoring compliance arrangements.

3.7 Documentation

54. Documentation of the results achieved by taking the steps set out in sections 3.3 to 3.7 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 effective and appropriate 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.

3.8 Relationship Risk Profile

55. Consideration of the information obtained during the relationship risk assessment

will enable a financial services business to establish a risk profile for each business relationship.

56. The creation of a risk profile of a particular business relationship, in conjunction with the information obtained in connection with compliance with the provisions of Rules in Chapters 4, 5 and 6 of the Handbook, will allow a financial services business to determine 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. The risk profile must contain information on three areas:

- the identity of the customer, beneficial owner and underlying principals;
- the purpose and intended nature of the business relationship; and
- the type, volume and value of activity that can be expected within the business relationship.

3.8.1 Business from Sensitive Sources Notices

57. When creating a relationship risk profile a financial services business must have regard to Business from Sensitive Sources Notices, which are issued from time to time by the Commission. These notices highlight potential risks arising from particular sources of business.

58. Care must be taken when dealing with customers 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.

59. 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.

3.8.2 Profile indicators

60. 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 risk 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 financial services 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;
- customers with private wealth, where the source is identified as legitimate; 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.

61. 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 risk 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;
- an individual who is a Politically Exposed Person (PEP) and/or association with a location which carries a higher exposure to the possibility of corruption;
- customers based in, or conducting business in or through, a Non Cooperative Country or Territory (NCCT) or a country or territory with known higher levels of corruption or organised crime, or involved in illegal drug production/ processing/distribution, or associated with terrorism;
- customers based in, or conducting business in or through, a country or territory which does not or insufficiently applies the FATF Recommendations;
- 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 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

- hold mail or retained mail arrangements;
- significant and/or frequent cash transactions;
- bearer shares and similar instruments; and
- inappropriate delegation of authority.

62. A financial services business must ensure that where, in a particular customer/product/service/delivery channel combination, any one aspect of the business relationship is considered to carry a high risk of money laundering or terrorist financing, the overall risk of the business relationship is treated as high risk.

CHAPTER 4 – CUSTOMER DUE DILIGENCE

Key Regulations

Sections in this chapter

CHAPTER 4 – CUSTOMER DUE DILIGENCE

Sections in this chapter **Page**

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 which the financial services business knows, or has reasonable cause to suspect, is 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) any customer shall be identified and his identity verified using identification data;

(b) any introducer or other 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) any 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 identity 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) Identification of the beneficiaries of a trust or other legal arrangement and verification of the identity of customers 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. (1) Where a financial services business can not comply with any of regulation 4(3)(a) to (d) it must, subject to paragraph (2) -

(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 report must be made pursuant to regulation 12(c).

(2) Where this regulation applies in the circumstances set out in regulation 4(2)(c), the business relationship or occasional transaction may be entered into or carried out in accordance with directions given by a police officer duly authorised for that purpose.

Regulation 10

10. (1) In the circumstances set out in paragraph (2), a financial services business may accept a written confirmation of identity 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, subject to limited exceptions provided for in Chapter 4 of the Handbook, keeps such identification data and documents.

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

(a) is an Appendix C financial services business; or

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

(i) the head office of both the introducer and the receiving financial services business fall within paragraph (2)(a); and

(ii) the introducer -

(A) where it is an overseas branch, is subject to effective policies, procedures and controls on countering money laundering and terrorist financing of the receiving financial services business; or

(B) where it is a member of the same group of companies, is subject to effective policies, procedures and controls on countering money laundering and terrorist financing of a common parent company to which the receiving financial services business is also subject.

(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 provided in the Handbook in considering compliance with the Regulations.

4.1 Objectives

63. 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 has been assessed as neither high nor low.

64. Where the risk of a particular business relationship has been assessed as high, 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.

65. Where the risk of a particular business relationship has been assessed as low 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

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

- constitute an essential part of risk management e.g. 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

67. 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.

68. 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 risk profile of the business relationship.

69. 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.

70. Financial services businesses must judge, on a risk-based approach, how much identification or 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.

71. 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), and provisions regulating the power to bind the legal person or arrangement.

72. 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

73. Sections 4.4 to 4.7 of this chapter provide rules and guidance on how to meet the identification and verification of identity requirements of Regulation 4.

74. 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.

75. For business relationships which have been identified as low risk see Chapter 6.

4.4.1 Identification data for individuals

76. 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 (e.g. 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

77. The legal name, address, date and place of birth, nationality and official personal identification number of the individual must be verified.

78. In order to verify the legal name, address, date and place of birth, nationality and official personal identification number 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.

79. The examples quoted above are not the only possibilities. In particular countries or territories 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

80. 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 financial services 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 financial services 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.

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

82. 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.

83. 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.

84. 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.

85. Where establishing a face-to-face business relationship with an individual customer

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

86. 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.

87. 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 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 Face-to-Face Individual Customers

88. At a minimum, in situations where non-Guernsey resident customers wish to establish a business relationship and it is not practical to obtain original documentation, a financial services business must obtain copies of identification data, which have been certified by a suitable certifier.

4.5.1 Suitable certifiers

89. 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 met the individual (where certifying evidence of identity containing a photograph) and have seen the original documentation.

90. The following is a list of examples of acceptable persons to certify evidence of identity which is not intended to be exhaustive:

- a member of the judiciary, a senior civil servant, or a serving police or customs officer;
- an officer of an embassy, consulate or high commission of the country or territory of issue of documentary evidence of identity;
- a lawyer or notary public who is a member of a recognised professional body;
- an actuary who is a member of a recognised professional body;
- an accountant who is a member of a recognised professional body; or
- a director or officer of an Appendix C financial services business (see the definition in Appendix C to the Handbook) or of a financial services business subject to group/parent policy where the Head Office is situated in a country or territory listed in Appendix C to the Handbook.

91. A financial services business must give consideration to the suitability of a certifier based on the assessed risk of the business relationship together with the level of reliance being placed on the certified documents and 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.

92. Where certified copy documents are accepted, it is the responsibility of the financial services business to satisfy itself, where possible, that the certifier is appropriate, for example, the certifier is not closely related to the person whose identity is being certified. In all cases, a financial services business must ensure that the customer's signature on the identification document matches the signature on the application form, or any other document in the possession of the financial services business.

93. A suitable certifier must certify that:

- he has seen original documentation verifying identity and residential address;
- the copy of the document (which he certifies) is a complete and accurate copy of that original; and
- where the document is to be used to verify identity of an individual and contains a photograph, the photograph contained in the document certified bears a true likeness to the individual requesting certification.

94. The certifier must also sign and date the copy identification data, and provide adequate information, e.g. name, position or capacity, and ideally address and a telephone number or e-mail address so that contact can be made in the event of a query.

4.5.2 Additional measures

95. Examples of adequate measures required by Regulation 5 in order to mitigate or manage the specific risks associated with non face-to-face business relationships or transactions include:

- 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 bank situated in a country or territory listed in Appendix C to the Handbook.

4.5.3 Verification of residential address of overseas residents

96. In respect of both face-to-face and non face-to-face business, 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.

97. 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 Non-Personal Customers

98. The identification and verification requirements in respect of non-personal customers are different from those for individuals as beneficial owners and underlying principals must also be identified. Although a non-personal customer 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.

99. 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 money laundering and terrorist financing risk established in the risk profile of the particular customer/product/service combination, a financial services business must consider the extent to which 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

100. This section identifies the requirements which are relevant to situations where a legal body, which is not regulated or registered on a regulated market, is the customer, a beneficial owner on whose behalf a customer is acting or an underlying principal.

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

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

103. When seeking to identify and verify the identity of beneficial owners, underlying principals, the directors 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.

104. The following 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;
- a copy of the Directors' Register;
- a copy of the Shareholders' Register;
- independent information sources, including electronic sources, e.g. 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.

105. Where the documents provided are copies of the originals the financial services business must ensure they are certified by the company secretary or equivalent officer.

106. 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, e.g. obtaining additional information or documentation.

107. 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.

108. Powers of attorney and similar third party mandates must attract suspicion if there is no evident reason for granting them. In addition, an unnecessarily wide-ranging scope to the mandate must also attract suspicion. 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 his behalf and verification must be undertaken on the holders of the powers of attorney as well as the customer. A financial services businesses must also ascertain the reason for the granting of the power of attorney.

4.6.2 Legal arrangements

109. 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.

110. 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.

4.6.3 Obligations of trustees

111. 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 to the best of the trustee's knowledge, likely to benefit from the trust.

112. Beneficiaries must be identified and their identity verified as soon as reasonably practicable. Where it is not possible to do this at the outset of the business relationship, identification and verification of beneficiaries must be undertaken prior to any distribution of trust assets to (or on behalf of) any beneficiary. The verification of identity of other underlying principals such as settlors, co-trustees and protectors must be carried out when the business relationship is established.

113. 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.

114. Where the relationship is a high risk relationship, trustees must consider whether additional verification checks are appropriate – see Chapter 5 on high risk relationships.

4.6.4 Obligations of financial services businesses dealing with trusts

115. Subject to section 6.6 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 financial services 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 who is, to the best of the trustee's knowledge, likely to benefit from the trust,

and either itself verify the identity of those persons or request the trustee to provide identification data on them, by way of a certificate or summary sheet (see Appendix F); 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.

116. 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 personal customers and legal bodies – see sections 4.4 and 4.6.1.

117. Where the business relationship (or any underlying principal) is a high risk relationship, a financial services business must consider what additional verification checks are appropriate – see Chapter 5 on high risk relationships.

4.7 Acquisition of a Business or Block of Customers

118. There are circumstances where a financial services business may acquire a business with established business relationships or a block of customers, e.g. by way of asset purchase.

119. 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.

120. 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 financial services 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.

121. 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.

4.8 Identification and Verification of Identity in Introduced Business Relationships

122. An introduced business relationship is where a financial services business is acting on behalf of one or more third parties who are also its customers and establishes

a business relationship on their behalf with another 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.

123. 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 4.10.

124. In the context of introduced business an intermediary business relationship is where an introducer, when establishing a relationship with another financial services business, meets the criteria necessary to be considered as an intermediary and can therefore be considered as the customer of the financial services business - see section 6.6.

125. 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 owner and any underlying principals.

126. In the circumstances set out in Regulation 10, a financial services business may accept 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).

127. A financial services business must also take adequate steps to be satisfied that the introducer itself retains and will make available upon request and without delay, the verification documentation and other evidence collected under the CDD process.

128. 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 must include 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.

129. 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. The financial services business must have a programme of testing to ensure that introducers are able to fulfil the requirement that identification data and other relevant documentation can be made available 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.

130. 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.

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

4.8.1 Group introducers

132. 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 4.8 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.

133. Group introduced business must not be regarded as intrinsically low risk. As identified in section 4.8 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.

4.8.2 Introductions within the Crown Dependencies

134. A Guernsey financial services business may accept introduced business from an institution ("the middle institution") which has received a certificate/summary sheet from the original introducer, which details the necessary information but where the middle institution does not itself hold copies of identification data and other relevant underlying documentation on the introduced client in the situation described in the next paragraph.

135. When accepting introduced business from a middle institution the following criteria must be met:

(a) the original introducer is regulated for the type of business being introduced;

(b) both introducers operate from Guernsey, Jersey or the Isle of Man;

(c) the certificate/summary sheet provided to the Guernsey financial services business details the necessary information and has been signed by both the original introducer and the middle institution, committing the original introducer to providing copies of identification data and other relevant documentation, upon request without delay, to the Guernsey financial services business; and

(d) The Guernsey financial services business has a programme of testing to ensure that relevant documentation can be made available from the original introducer upon request without delay.

136. This procedure has the benefits of:

(a) avoiding the need in these specific circumstances, for more than one financial services business to hold the copies of identification data and other relevant documentation;

(b) avoiding the need in these specific circumstances, for the provision of two separate certificates/summary sheets; and

(c) avoiding the establishment of a direct commercial business relationship between the original introducer and the Guernsey financial services business.

4.9 Chains of Introducers

137. Sections 4.8, 4.8.1 and 4.8.2 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.

138. The circumstances described in section 4.8.2 would not be seen by the Commission as a chain because the Guernsey financial services business is aware of the identity of both the introducers and, if necessary, could approach the original introducer directly in order to obtain copies of identification data and other relevant documentation, upon request without delay, should the need arise.

139. 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.

4.10 Pooled Bank Accounts

140. 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 6.6 provides information on the identification and verification requirements of such relationships.

141. Where the pooled account is held on behalf of a professional firm or a financial services business which is not regulated or where the institution does not meet the requirements as set out in section 6.6 and the product or service is not a product or service set out in section 6.6.2, 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.

4.11 Timing of Identification and Verification of Identity

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

143. 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 effective and appropriate policies, procedures and controls in place so as to manage the risk which must include:

- establishing that it is a low 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.

4.11.1 Occasional transactions

144. 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. For the purposes of the Handbook, transactions, which are 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.

4.12 Failure to Complete Identification or Verification of Identity

145. When a financial services business has had to terminate a business relationship (e.g.

close an account) or has been unable to open an account, commence a business relationship or perform any transactions as a result of being unable to complete identification or verification procedures, it should make an assessment of the circumstances.

146. Where the business relationship has commenced and a financial services business is unable to complete verification of identity, a financial services business must terminate the business relationship in accordance with Regulation 9 and in so doing must return any funds held to the customer's order and make an assessment of the circumstances. Funds must never be returned to a third party but only to the source from which they came.

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 where the customer is established or situated in a country or territory -

(i) that does not apply or insufficiently applies the Financial Action Task Force Recommendations on Money Laundering; or

(ii) in respect of which the Commission considers there to be a high risk; and

(d) a business relationship or an occasional transaction which has been assessed as a high risk relationship pursuant to regulation 3(1)(c).

(2) In paragraph (1) -

(a) "enhanced customer due diligence" means additional steps in relation to identification and verification to those required under regulation 4(3) including taking the following steps -

(i) considering whether additional identification data needs to be obtained;

(ii) considering whether additional aspects of the customer's identity need to be verified;

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

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

(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) Where a business relationship falls within paragraph (1)(a), a financial services business must ensure that senior management approval is obtained for establishing, or, in the case of an existing business relationship, continuing that relationship.

(4) Where the customer was not physically present 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 provided in the Handbook in considering compliance with the Regulations.

5.1 Objectives

147. This chapter provides for the treatment of business relationships 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 the creation of risk assessments and risk profiles and with Chapter 4 which provides for the standard CDD requirements.

5.2 Enhanced Policies, Procedures and Controls

148. Where a financial services business has assessed 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

149. 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.

150. 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 effective and appropriate policies, procedures and controls in place to ensure compliance with the enhanced due diligence requirements of Regulation 5.

5.3.1 Source of funds and source of wealth

151. 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.

152. Understanding the customer's source of funds and source of wealth are important aspects of CDD especially in high risk relationships.

153. A financial services business must, in establishing the source of any funds or

wealth, consider 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

154. 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.

155. 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 identification and verification 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, effective and appropriate;
- 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.

156. 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 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.

157. Financial services businesses must, pursuant to Regulation 15(a), have effective and appropriate policies, procedures and controls to ensure that correspondent relationships are only established with foreign banks and other institutions that are supervised for AML/CFT purposes and that operate from Guernsey or countries or

territories listed in Appendix C to the Handbook.

158. Additionally, a financial services business must have effective and appropriate 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

159. In addition to the enhanced CDD measures required by Regulation 5 for high risk relationships, financial services businesses must, pursuant to Regulation 15(a), have effective and appropriate policies, procedures and controls in place to 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, terrorism, terrorist financing and other organised crime.

160. Financial services business must have effective and appropriate procedures in place which include:

- having effective measures in place to ensure they are aware of concerns about weaknesses in the AML/CFT systems of other countries or territories;
- referral to senior management prior to establishing relationships from such countries or territories;
- identifying transactions which (in the context of business relationships and occasional transactions) have no apparent economic or visible lawful purpose and examining the background and purpose of such transactions; and
- recording in writing the findings of such examinations in order to assist the Commission, the FIS and other domestic competent authorities.

161. 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 issued from time to time by the Commission;
- findings of reports issued by the FATF, FATF-style regional bodies, the Offshore Group of Banking Supervisors, Transparency International, the International Monetary Fund and the World Bank; 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 Shares

162. As identified in section 3.8.2 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.

163. 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 identification and verification requirements of Regulation 4 are met and that legal persons who have issued or have the potential to issue bearer shares 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(1)(c), 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 -

(a) in accordance with the requirements set out in Chapter 6 of the Handbook; and

(b) provided that the customer and every beneficial owner and underlying principal is established or situated in the Bailiwick or a country or territory listed in Appendix C to the Handbook.

(3) For the avoidance of doubt, simplified or reduced customer due diligence shall not be applied -

(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 provided in the Handbook in considering compliance with the Regulations.

6.1 Objectives

164. This chapter provides for the treatment of relationships which have been assessed pursuant to Regulation 3 as low risk relationships and should be read in conjunction with Chapter 3 of the Handbook, which provides guidance on factors to consider when preparing a risk assessment and a risk profile and Chapter 4 which provides for necessary CDD measures.

6.2 Simplified or Reduced CDD Measures

165. 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 owner and any underlying principals. Nevertheless, there are circumstances where the risk of money laundering or terrorist financing is low (for example, locally resident retail customers who have a business relationship which is understood by the financial services business), or where information on the identity of the customer, beneficial owner and underlying principals is publicly available, or where adequate checks and controls exist elsewhere in national systems.

166. 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 owner and underlying principals.

167. A financial services business must ensure that should any material change in circumstances 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.

168. 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.

169. 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. Where a financial services business has the slightest doubt that any aspect of the relationship or occasional transaction could be other than low (e.g. by virtue of the country or territory or value of the relationship) then simplified or reduced CDD measures must not be applied – see Chapter 3 on the risk-based approach.

6.2.1 Identification data for face-to face individuals

170. Where establishing a face-to-face business relationship with an individual customer 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 and any other names used (such as maiden name);
- current permanent address; and
- date, place of birth and nationality.

6.2.2 Verification of identity for face-to-face individuals

171. The legal name and either the current permanent address or the date and place of birth of the individual must be verified.

172. In order to verify the legal name and either the current permanent address or date and place of birth, the following documents are considered to be the best possible, in decending order of acceptability:

- 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.

6.3 Receipt of Funds as Verification of Identity

173. Where the customer, beneficial owner and any underlying principal have been identified and the product or service is such that the relationship or occasional transaction is considered to be a low risk relationship then the receipt of funds may be considered to provide a satisfactory means of verifying identity where:

- all initial and future funds are received from an Appendix C financial services 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.

174. 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.

175. 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.

176. 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 identify of the customer, beneficial owner or underlying principal.

6.4 General Insurance – Commercial and Personal Lines business

177. With reference to general insurance – commercial and personal lines business, insurance intermediaries licensed under the Insurance Managers and Insurance Intermediaries (Bailiwick of Guernsey) Law, 2002 must have appropriate and effective policies, procedures and controls in place to assess, manage and mitigate the risk of the business relationship or occasional transaction.

6.4.1 Receipt of funds

178. Where a licensed insurance intermediary has identified the customer and any beneficial owner or underlying principal the receipt of funds may be considered as a satisfactory means of verifying such identity, where all the following criteria are met:

- the product or service is such that the relationship is considered to present a low risk of money laundering and terrorist financing;
- all initial and future funds are received from an Appendix C financial services 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 and any beneficial owners or underlying principals; and
- no payments may be received from third parties.

179. A licensed insurance intermediary must ensure that, once a relationship has been established, should any of the above conditions no longer be met then verification of identity must be carried out in accordance with Chapter 4 of the Handbook.

180. Should a licensed insurance intermediary have reason to question the motives behind

a particular transaction or believe that the business relationship is being structured to avoid the standard identification requirements, it must not permit the use of the receipt of funds as verification of the identity of the customer any beneficial owner or underlying principal.

6.4.2 Making payments

181. Subject to the following paragraph, prior to a payment being made, additional verification must be completed in order for the licensed insurance intermediary to be satisfied of the identity of the recipient of such a payment. Such additional verification must be appropriate to the assessed risk of the relationship.

182. A licensed insurance intermediary is not required to undertake additional verification when a payment is to be made and the relationship is such that:

- business has been introduced to the licensed insurance intermediary by a third party (other than the customer or any beneficial owner or underlying principal), and the licensed insurance intermediary has satisfied itself as to the suitability of the third party; or
- all payments (ie return premiums and claims payments) to the customer, any beneficial owner or underlying principal or third party are made by the insurance company (ie not the licensed insurance intermediary) and, therefore, the AML/CFT risk is that of the insurance company rather than the licensed insurance intermediary; or
- payment of claims is approved by an independent professional third party such as a loss adjuster or lawyer acting for the insurer.

6.5 Appendix C Financial Services Businesses

183. When the customer is an Appendix C financial services business (see the definition in Appendix C to the Handbook), verification of the identity of the financial services business is not required. However, if the financial services business is acting for underlying principals then those underlying principals would need to have their identity verified in accordance with the requirements of the Handbook.

184. 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 financial services business (see the definition in Appendix C to the Handbook) it is not necessary to identify and verify the identity of such persons. For example, a director (or equivalent) of a Guernsey fiduciary which is acting as trustee.

6.6 Where an Introducer can be Considered to be an Intermediary

185. Section 4.8 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.

186. There are occasions, see sections 6.6.1 and 6.6.2, where a specific range of criteria are met and an introducer can be considered to be an intermediary. As such the intermediary can be treated as the customer of the financial services business in relation to the CDD requirements in Regulation 4 and Chapter 4 and the business relationship may be assessed as a low risk relationship pursuant to Regulation 3 and Chapter 3.

187. Where the financial services business in Guernsey wishes to consider the introducer to be an intermediary it must prepare and retain documentary evidence of the following:

- the adequacy of its process to determine the risk of the business relationship with the introducer;
- the reasonableness of its conclusions that it is a low risk relationship;
- that it has undertaken CDD procedures in respect of the introducer – see section 6.6.1; and
- that the product/service being provided meets the requirements of section 6.6.2.

6.6.1 CDD procedures on the introducer

188. Where the financial services business in Guernsey wishes to consider the introducer to be an intermediary so it may be treated as its customer, the financial services business must undertake CDD procedures in respect of the introducer to ensure that the introducer:

- is an Appendix C financial services business (see the definition in Appendix C to the Handbook); or
- is 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 only and where the funds received by the firm have been received from a bank operating in Guernsey or from a country or territory listed in Appendix C of the Handbook; and
- in either of the above cases, has provided a written confirmation to the financial services business which:
  - confirms that the introducer has appropriate risk-grading procedures in place to differentiate between the identification and verification requirements for high and low risk relationships;
  - contains adequate assurance that the introducer conducts the necessary identification and verification procedures in respect of its customers;
  - contains sufficient information to enable the financial services business to understand the purpose and intended nature of the business relationship;

- contains an assurance that no business relationships will be established where the introducer has considered the risk of money laundering or terrorist financing to be other than low e.g. there are no PEPs in the business relationship; and
- confirms that the account will only be operated by the introducer.

189. Where instructions are taken from the customer of the introducer or if the above criteria are not completely satisfied or are no longer met then the introducer can no longer be considered as an intermediary and treated as the customer and full CDD procedures as identified in Chapter 4 must take place in respect of the customer of the introducer and of the business relationship.

6.6.2 Products and services

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

Product/service	Introducer who may be considered to be an intermediary and treated as the customer
Where the shares of a company are traded on a regulated market or it is a subsidiary of such a company.	The company.
Employee benefit trusts which are set up by an employer for the benefit of employees (including directors) and former employees, their spouses and dependants and where the scheme rules do not permit the assignment of members' interests.	The sponsoring employer, the trustee and any other person who has control over the business relationship, e.g. the administrator or the product manager.
Employee share option plans.	The sponsoring employer, the trustee and any other person who has control over the business relationship, e.g. the administrator or the product manager.
Pension schemes established by employers – excluding retirement annuity trust schemes, private or personal pension schemes or small self-administered pension schemes.	The sponsoring employer, the trustee and any other person who has control over the business relationship, e.g. the administrator or the product manager.

Product/service	Introducer who may be considered to be an intermediary and treated 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.
Insurance policies where there is no cash-in value and where professional and independent third parties (such as loss adjusters) are satisfied before payments are made, e.g. kidnap and ransom insurance.	The regulated insurance broker.
Reinsurance to an insurer who in turn is issuing policies on a commercial basis only, where the reinsurance contract is arranged exclusively between the reinsurer and a recognised and properly regulated insurer and not between the reinsurer and any other party.	The insurer.
Investments via discretionary or advisory investment managers of their customers' monies into an open-ended collective investment fund regulated by the Commission.	The regulated financial services business, i.e. the discretionary or advisory investment manager.
Investments via discretionary or advisory investment managers of their customers' monies into a Guernsey closed-ended investment fund administered by a financial services business regulated by the Commission.	The regulated financial services business, i.e. the discretionary or advisory investment manager.

Product/service	Introducer who may be considered to be an intermediary and treated as the customer
The execution of investment instructions, e.g. the purchase or sale of securities on behalf of customers including the short-term holding of settlement proceeds on deposit.	The regulated financial services business providing the service.
Client accounts held by banks in the name of a licensed fiduciary or a professional firm where the holding of funds in the client account is on a short-term basis and is necessary to facilitate a transaction. Licensed fiduciaries should ensure that any such use is compatible with relevant trust deeds, and applicable legislation and Codes of Practice.	The professional firm or financial services business.

191. The Commission has based this list on risks of potential money laundering and terrorist financing.

192. 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.

CHAPTER 7 – WIRE TRANSFERS

Applicable Ordinances

Sections in this chapter

ORDINANCE

In addition to the Regulations, and the Rules and Guidance elsewhere in the Handbook, there are also dedicated Ordinances which provide for the treatment of wire transfers.

Financial services businesses must comply with the Transfer of Funds (Guernsey) Ordinance, 2007 and the parallel Ordinances applicable in Alderney and Sark and 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 Ordinances and the Regulations.

The text of the Ordinance is set out in Appendix E. That text is definitive. References to an "Ordinance" in this chapter will refer to the Ordinance relevant to the Island from which the institution is operating.

7. WIRE TRANSFERS

A financial services business must comply with the Ordinance, the Regulations and the Rules. In order to assist financial services businesses to understand the contents of the Ordinance, much of the text below paraphrases the policies, procedures and controls which are required by the Ordinance to be established and maintained. Any paraphrasing of that text within this chapter represents the Commission's own explanation of the Ordinance and is for the purposes of information and assistance only. That paraphrasing does not detract from the legal effect of the Ordinance 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 in order to meet the requirements of the Ordinance are in shaded boxes.

7.1 Objectives

193. This chapter provides for a payment service provider (PSP) to have clear and comprehensive policies, procedures and controls for ensuring that it has the ability to trace all wire transfers back to the originator of the transfer.

7.2 Scope

194. The requirements summarised in this chapter apply to transfers of funds in any currency sent or received by a PSP established in Guernsey.

195. The requirements do not apply to the transfers set out in the Schedule to the Transfer of Funds Ordinance.

196. References to the British Islands in this chapter are to the area that comprises the United Kingdom, Guernsey, Jersey and the Isle of Man.

197. There are different requirements in relation to transfers between financial services businesses within the British Islands and to transfers where the PSP of the payer or the payee is outside the British Islands.

7.3 Outgoing Transfers

198. Section 7.3.1 of this chapter summarises the procedures to be undertaken for non-account holders and section 7.3.2 summarises the procedures to be undertaken for account holders.

7.3.1 Transfers for non-account holders

199. In accordance with section 2 of the Ordinance, where a transfer of funds is not made from an account and the PSP is seeking to make a transfer in excess of €1,000 in a single transaction or in a linked series of transactions which are together in excess of

€1,000, it must obtain customer identification information on the payer and verify and record that information.

200. Where the transfer is at or below the €1,000 threshold then customer identification information on the payer must be obtained and recorded but it is not necessary to verify the customer information.

201. Where the transfer is being made to a PSP in the British Islands, the transfer must, in accordance with section 3(1) of the Ordinance, include a unique identifier (which can trace a transaction back to the customer). If further information e.g. the name and address of the payer is requested by the PSP of the payee, such information must be provided within three working days of the receipt of a request for such information.

202. Where the transfer is being made to a PSP in any other country or territory, section 2 of the Ordinance requires such transfers to include the following customer identification information (complete information):

- the name of the payer;
- a unique identifier (which can trace a transaction back to the customer); and
- the payer's address (residential or postal) which may be substituted with his date and place of birth (where relevant), his customer identification number or national identity number.

203. A customer identification number may be an internal reference number that is created by a PSP which uniquely identifies a payer (rather than an account that is operated for a payer), and which will continue throughout a business relationship, or it may be a number that is contained within an official document.

7.3.2 Transfers for account holders

204. In accordance with section 2 of the Ordinance where a PSP is seeking to make a transfer from an account, PSPs must:

- obtain customer identification information on the payer, verify that information, and record and retain that information; or
- have undertaken customer identification and verification procedures and retained records in connection with the opening of that account in accordance with the requirements of the Regulations and the Handbook,

but where the payer is an existing customer the PSP may deem verification to have taken place if it is appropriate to do so taking into account the risk of money laundering or terrorist financing.

205. Where the transfer is being made to a PSP in the British Islands, section 3 of the Ordinance requires such transfers to include a customer account number. The account

number could be, but is not required to be, expressed as the International Bank Account Number ("IBAN"). If further information e.g. the name and address of the payer is requested by the PSP of the payee, such information must be provided by the PSP within three working days of the receipt of a request for such information.

206. The provision which allows transfers being made to a PSP in the British Islands to only include a customer account number arises from expediency, not principle, in order to accommodate transfers by domestic systems like BACS which are currently unable to include complete information. Accordingly, where the system used for a transfer in the British Islands has the functionality to carry complete information, it may make sense to include it, and thereby reduce the likely incidence of inbound requests from payee PSPs for complete information.

207. Where the transfer is being made to a PSP in any other countries or territories, the transfer must include the following customer identification information:

- the name of the payer;
- the payer's account number (or IBAN); and
- the payer's address (residential or postal), which may be substituted with his date and place of birth (where relevant), his customer identification number or national identity number.

208. In the case of a payer that is a company, the transfer must include the address at which the company's business is conducted. In the case of a payer that is a trustee, a transfer must be accompanied by the address of the trustee.

209. 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 financial services business, the transfers are accompanied by the customer identification information necessary to meet the requirements of the Ordinance.

210. Where a PSP is itself the payer (i.e. acting as principal), as will sometimes be the case even for SWIFT MT102 and 103 messages, the requirement to provide name, address, and account number may be met by the provision of the Bank Identifier Code (BIC), although an account number must be included where this is available. Where a Business Entity Identifier (BEI) accompanies a transfer, the account number must always be included.

7.3.3 Batch files – transfers either inside or outside the British Islands

211. In accordance with section 4 of the Ordinance, batch files from a single payer to multiple payees must carry the information identified in sections 7.3.1 and 7.3.2 of this chapter for the payer (which will depend on whether the PSP of a payee is located within or outside the British Islands). However, the individual transfers within the batch file need only carry the payer's customer account number (or unique customer identifier if there is no account number).

7.3.4 Minimum standards

212. The information requirements of section 7.3 of this chapter 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.

213. In order to ensure that information provided under the Ordinance is also processed in line with the Data Protection (Bailiwick of Guernsey) Law, 2001, it may be advisable for a payer PSP to ensure that its terms and conditions of business with each payer include reference to the information that it may provide under the requirements set out in sections 2 and 3 of the Ordinance.

7.4 Incoming Transfers

214. Sections 5 and 6 of the Ordinance require PSPs to have effective policies, procedures and controls for checking that incoming payments contain the required customer identification information (which will depend on whether the payer's PSP is located within or outside the British Islands) – see sections 7.3.1 and 7.3.2 of this chapter.

7.4.1 Detection of missing or incomplete information

215. 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 e.g. by undertaking sample testing to identify fields containing incomplete information on the payer and, where information is incomplete, to take specified action.

216. SWIFT payments on which mandatory payer 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 is not present at all. However, it is accepted that where the payer information fields are completed with incorrect or meaningless information, or where there is no account number, the payment will pass through the system. SWIFT is currently considering how its validation standards might be improved to respond more effectively to the requirements of FATF Special Recommendation VII. 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.

217. Under section 5 of the Ordinance a PSP of a payee must:

- detect whether or not the fields relating to information on the payer have been completed in accordance with the characters or inputs admissible within the conventions of the messaging or payment and settlement system, i.e. ensure that validation rules of whichever messaging or payment system used are being utilised; and
- have effective procedures in place to detect the absence of required information on the payer.

218. PSPs must therefore have in place effective and appropriate policies, procedures and controls which subject incoming payment transfers to an appropriate level of post-event random sampling in order to detect non-compliant payments.

219. The level of the sampling must be appropriate to the risk of the financial services business being used in connection with money laundering and terrorist financing and consideration should be given to areas such as:

- the value of the transaction;
- the country or territory of the payer; and
- 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.

220. Undertaking such an assessment will allow the PSP to make a considered decision as to the appropriate action to be taken.

221. Under section 6 of the Ordinance if a PSP has identified in the course of processing a payment that information on the payer is missing or incomplete it must either;

- reject the transfer; or
- ask for complete information on the payer; or
- take such other steps as the Commission may by order direct,

but must comply with any other relevant provision of an enactment relating to money laundering or terrorist financing if that provision is contrary to the requirement to provide missing or incomplete information or imposes additional requirements, e.g. compliance with tipping off provisions.

222. A PSP should take a risk-based approach when considering the most appropriate course of action to be taken. Dependent on the circumstances, in addition to the options set out in the above paragraph, examples of other appropriate action could include making the payment or holding the funds and advising the MLRO of the payee's PSP.

223. Where a payee PSP becomes aware subsequent to processing the payment that information on the payer 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 necessary information on the payer; and/or
- take any other action which the Commission may by order direct.

7.4.2 Failure to supply information on a regular basis

224. Section 6 of the Ordinance also sets out the action required where a PSP regularly

fails to supply information on the payer required by the Ordinance.

225. In order to comply with the requirements of section 6 of the Ordinance, 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 and the FIS of that fact and take steps to attempt to ensure that such information is supplied. The 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.

7.4.3 Reporting of suspicion

226. In accordance with section 7 of the Ordinance, where information on the payer accompanying a transfer of funds is missing or incomplete, the PSP of the payee must take this into account in assessing whether the transfer of funds, or any related transaction, is suspicious, and whether a disclosure should be made to the FIS in accordance with the legislative requirements referred to in Chapter 10 of the Handbook.

7.4.4 Record keeping

227. Section 7 of the Ordinance requires the PSP of the payee to retain all records of any information received on the payer of a transfer of funds for five years from the date of the transfer of funds.

228. More information on record keeping is available in Chapter 12 of the Handbook.

7.5 Intermediary Payment Service Providers

229. In accordance with sections 8 and 9 of the Ordinance, intermediary PSPs, (e.g. those acting as agents for other payment service providers or who provide correspondent banking facilities) must, subject to technical limitations, ensure that all information received on a payer which accompanies a wire transfer is retained with the transfer.

230. Where an intermediary PSP uses a payment system with technical limitations (i.e. which prevents information on the payer accompanying transfers of funds) for transfers, and is aware that payer information is missing or incomplete it must:

- notify the PSP of the payee that the information is missing or incomplete through a procedure agreed between the intermediary and the PSP; and
- retain records of all information received on the payer for 5 years from the date of the transfer.

231. If requested to do so by the PSP of the payee, the intermediary PSP must provide the PSP of the payee with all information it has received on the payer within three working days of receiving the request.

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.
- Regulations 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 names which it knows, or has reasonable cause to suspect, to be fictitious; 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, to ensure compliance with the Financial Action Task Force Recommendations on Money Laundering and other international requirements, in relation to all

aspects of a banking group's business carried on worldwide and in accordance with the Core Principles of Effective Banking Supervision issued by the Basel Committee on Banking Supervision;

(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 unafilliated with a banking group 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 provided in the Handbook in considering compliance with the Regulations.

8.1 Objectives

232. 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

233. 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 risk profile of a particular business relationship which in turn will allow the financial services business to determine the extent of identification information (and other CDD information) which is required.

234. 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.

235. Each financial services business is best placed to assess the risk profile 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

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

- 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.

237. 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

238. Financial services businesses may, as a result of the Commission's Statement on Anti-Money Laundering Standards for Existing Customers, which was issued in June 2004, have already undertaken effective and appropriate CDD procedures which meet the requirements of the Regulations and the Handbook in respect of existing customers. In these circumstances such financial services businesses are not required to introduce a further retrospective know your customer programme.

239. In order to meet the requirements of Regulation 4(1)(b) , where a financial services business has not introduced or completed a retrospective know your customer programme, effective and appropriate CDD procedures on existing customers must be undertaken on the basis of materiality and risk at appropriate times.

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) on going customer due diligence which shall include 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 provided in the Handbook in considering compliance with the Regulations.

9.1 Objectives

240. 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

241. 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.

242. Monitoring of the activity of a business relationship must be carried out on the basis of a risk-based approach, with high risk customer/product/service/delivery channel combinations being subjected to an appropriate frequency of scrutiny, which must be greater than may be appropriate for low risk combinations

243. Such 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 and risk profile, and where necessary, the source of funds.

244. 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.

245. 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.

246. 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

247. 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.

248. 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.

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

250. A larger or more complex financial services business may also demonstrate ongoing monitoring through the use of computerised systems. For example 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.

251. 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

252. 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.

253. 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.

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

CHAPTER 10 – REPORTING SUSPICION

Additional legislation

Key Regulations

Sections in this chapter

ADDITIONAL LEGISLATION

In addition to the Regulations, rules and guidance in the Handbook there are two 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 and the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002, and 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:

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

Section 15 of the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002. [To be amended]

Sections 1 and 2 of the Disclosure (Bailiwick of Guernsey) Law, 2007 [latest draft]

Failure to disclose knowledge or suspicion etc. of money laundering - financial services businesses.

1. (1) A person commits an offence if each of the following conditions is satisfied.

(2) The first condition is that he -

(a) knows or suspects, or

(b) has reasonable grounds for knowing or suspecting,

that another person is engaged in money laundering.

(3) The second condition is that the information or other matter -

(a) on which his knowledge or suspicion is based, or

(b) which gives reasonable grounds for such knowledge or suspicion,

came to him in the course of the business of a financial services business.

(4) The third condition is that he does not make the required disclosure as soon as is practicable after the information or other matter comes to him.

(5) The required disclosure is a disclosure of the information or other matter -
(a) to a nominated officer or a police officer,

(b) in the form and manner (if any) prescribed for the purposes of this subsection by regulations under section 11.

(6) But a person does not commit an offence under this section if-

(a) he has a reasonable excuse for not disclosing the information or other matter,

(b) he is a professional legal adviser and the information or other matter came to him in privileged circumstances, or

(c) subsection (7) applies to him.

(7) This subsection applies to a person if -

(a) he does not know or suspect that another person is engaged in money laundering, and

(b) he has not been provided by his employer with such training as is required by regulations made under section 49 of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 .

(8) In deciding whether a person committed an offence under this section the court must consider whether he followed any relevant rules or guidance which were at the time concerned -

(a) made or issued by the Commission under section 15 or any other enactment, and

(b) published in a manner it approved as appropriate in its opinion to bring the rules or guidance to the attention of persons likely to be affected by it.

(9) A disclosure to a nominated officer is a disclosure which -

(a) is made to a person nominated by the alleged offender's employer to receive disclosures under this section, and

(b) is made in the course of the alleged offender's employment and in accordance with the procedure established by the employer for the purpose.

(10) For the purposes of a disclosure to a nominated officer -

(a) references to a person's employer include any body, association or organisation (including a voluntary organisation) in the course of the business of which the person carries out a function (whether or not for gain or reward), and

(b) references to employment are to be construed accordingly.

(11) Information or another matter comes to a professional legal adviser in privileged

circumstances if it is communicated or given to him -

(a) by (or by a representative of) a client of his in connection with the giving by the adviser of legal advice to the client,

(b) by (or by a representative of) a person seeking legal advice from the adviser, or

(c) by a person in connection with legal proceedings or contemplated legal proceedings.

(12) But subsection (11) does not apply to information or another matter which is communicated or given with a view to furthering a criminal purpose.

(13) A disclosure to a nominated officer or to a police officer does not contravene any obligation as to confidentiality or other restriction on the disclosure of information imposed by statute, contract or otherwise.

Failure to disclose knowledge or suspicion etc. of money laundering - nominated officers in financial services businesses.

2. (1) A person who is a nominated officer under section 1(9)(a) commits an offence if the conditions in subsections (2) to (4) are satisfied.

(2) The first condition is that he -

(a) knows or suspects, or

(b) has reasonable grounds for knowing or suspecting,

that another person is engaged in money laundering.

(3) The second condition is that the information or other matter -

(a) on which his knowledge or suspicion is based, or

(b) which gives reasonable grounds for such knowledge or suspicion,

came to him in consequence of a disclosure made under section 1.

(4) The third condition is that he does not make the required disclosure as soon as is practicable after the information or other matter comes to him.

(5) The required disclosure is a disclosure of the information or other matter -

(a) to a police officer,

(b) in the form and manner (if any) prescribed for the purposes of this subsection

by regulations under section 11.

(6) But a person does not commit an offence under this section if he has a reasonable excuse for not disclosing the information or other matter.

(7) In deciding whether a person committed an offence under this section the court must consider whether he followed any relevant rules or guidance which were at the time concerned -

(a) made or issued by the Commission under section 15 or any other enactment, and

(b) published in a manner it approved as appropriate in its opinion to bring the rules or guidance to the attention of persons likely to be affected by it.

(8) A disclosure to a police officer does not contravene any obligation as to confidentiality or other restriction on the disclosure of information imposed by statute, contract or otherwise.

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 a police officer 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 effective and appropriate procedures and controls as are necessary to ensure compliance with 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 provided in the Handbook in considering compliance with the Regulations.

10.1 Objectives

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

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

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

10.2 Obligation to Report

258. 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.

259. 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 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 media, intermediaries, or the customer himself.

260. A financial services business must establish effective and appropriate 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;
- 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 he discloses that suspicion to the FIS – see section 10.4; and

- where, during the customer identification and verification 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.

261. 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.

262. 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.

263. 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.

264. 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.

265. 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

266. A financial services business must have effective and appropriate 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.

10.4 Form and Manner of Disclosing to the FIS

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

268. 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.

269. Disclosures must to be made in the standard form set out in Appendix D2. [This form will be prescribed in Regulations made by the Home Department under the Disclosure Law and the Terrorism and Crime Law.] The disclosure may be delivered by post, fax or e-mail and its receipt will be acknowledged by the FIS in writing. The means of delivery is at the discretion of the financial services business and subject to its security protocols. If a disclosure is sent by fax or e-mail there is no requirement to send a duplicate disclosure via post.

270. The financial services business should provide as much information and documentation (e.g. 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.

271. When considering the provision of information to the FIS a financial services business should be aware of the Money Laundering (Disclosure of Information) (Guernsey) Law, 1995, the Money Laundering (Disclosure of Information) (Alderney) Law, 1998 and the Money Laundering (Disclosure of Information) (Sark) Law, 2001 which state:

"No obligation of secrecy or confidence or other restriction on the disclosure of information to which any person may be subject, whether arising by statute, contract or otherwise, shall be regarded as being contravened by reason of disclosure by that person or by any of his officers, servants or agents to an officer of:

(a) any reasonable suspicion or belief that any money or other property is, or is derived from or represents, the proceeds of criminal activity;

(b) any information or document relating to:

(i) any such money or property;

(ii) any transaction concerning it;

(iii) the parties to any such transaction; and

(c) any fact or matter upon which any such suspicion or belief is based."

272. In the context of these three laws a financial services business should note that the reference to an "officer" includes a police or customs officer, or an officer of the Commission – see section 10.8.

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

274. 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.

275. 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.

276. 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.

277. A financial services business should develop its own contacts with the FIS and periodically discuss with the FIS the nature of suspicions which should or should not be disclosed.

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

10.5 The Response of the FIS

279. The receipt of a disclosure will be promptly acknowledged in writing by the FIS.

280. 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.

281. 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. On receipt of such a request the FIS will consider whether or not it may give consent under the relevant provisions of the Proceeds of Crime or Terrorism and Crime Laws. Any consent given will be in writing and will specify the transaction or activity to which the consent relates. In urgent matters, consent may be given orally by the FIS, but will be followed by written confirmation.

282. 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.

283. 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.

284. The FIS may, on occasions, seek additional information from the disclosing financial services business. Such additional information includes financial, administrative and law enforcement 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. [The Law Officers and the FIS propose that the Disclosure Law and the Terrorism and Crime Law should permit the Home Department to make Regulations on the provision of such additional information to the FIS.]

285. 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

286. Once an internal suspicion report to a MLRO or a disclosure to the FIS has been made, where required under the Disclosure Law or Terrorism and Crime Law, it is a criminal offence for anyone to release information which is likely to prejudice an investigation.

287. 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. For an offence to be committed, tipping off must

invariably be undertaken knowing or suspecting a disclosure has been made and the offence is committed where information is disclosed to, as opposed to requested from, a third party.

288. 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.

289. 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 commercial decision for the financial services business.

10.7 Terminating a Business Relationship

290. Whether or not to terminate a business relationship is a commercial decision except where required by legislation, e.g. where the financial services business cannot obtain required CDD information (see Chapter 4 and Regulation 9) or where continuing with the relationship would involve the financial services business committing an offence under, e.g. the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 or the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002.

291. Where a financial services business subsequently makes a decision to terminate a business relationship where they have previously made a disclosure or requested consent, it should update the FIS and consider whether it is necessary to request consent under the relevant legislative requirements in respect of any transaction or activity necessary to terminate the business relationship.

10.8 Reports to the Commission

292. In addition to disclosing to the FIS, financial services businesses should at the same time make such disclosures to the Commission, where:

- the policies, procedures and controls of the financial services business failed to detect the transaction or activity and the matter had been brought to the attention of the financial services business in another way (e.g. by the FIS) – unless the FIS has specifically requested that such information should not be communicated to another person;
- the transaction or activity may present a significant reputational risk to Guernsey and/or the financial services business;
- it is suspected that an employee of the financial services business was involved; or
- an employee of the financial services business has been dismissed for serious breaches of its internal policies, procedures and controls.

293. Disclosures to the Commission should be in the same format as those provided to the FIS.

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 effective and appropriate 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; and

(c) the implications of non-compliance by employees with any rules or guidance 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 provided in the Handbook in considering compliance with the Regulations.

11.1 Objectives

294. 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

295. 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 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; and
- requesting information from the employee with regard to any criminal convictions and the provision of a check of his criminal record (in accordance with legislation, i.e. concerning Rehabilitation of Offenders)

296. 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

297. 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.

298. 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

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

300. 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.

301. 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 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

302. 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 and any nominated persons or 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;
- liaising with law enforcement agencies; and
- the management of the risk of tipping off.

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

11.4.2 The Board and senior management

304. 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.

305. 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:

- all aspects 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

306. As part of providing comprehensive ongoing training, induction training must be provided for all new relevant employees prior to them becoming actively involved in day-to-day operations, and 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.

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

- the principal vulnerabilities of any new products and services 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.

308. 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.

11.6 The Relevance of Training

309. 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 best practice. The training should equip staff in respect of their responsibilities.

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

311. 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.

312. 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.

313. 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) Documents (including copies) and customer due diligence information 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 to any police officer, the Commission or any other person where such documents or customer due diligence information are requested pursuant to these Regulations or any relevant enactment.

(3) 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 or customer due diligence information so provided.

(4) A financial services business shall also keep records of -

(a) any reports made to a money laundering reporting officer under regulation 12 for five years starting from -

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

(ii) in the case of a report 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.

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 provided in the Handbook in considering compliance with the Regulations.

12.1 Objectives

314. 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

315. To ensure that the record keeping requirements of the Regulations are met, a financial services business must have effective and appropriate policies, procedures and controls in place to require that records are (where necessary) 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.

12.2.1 Customer due diligence information

316. In order to meet the requirement in the Regulations to keep transaction documents and identification data 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
- information as to where copies of the identification data may be obtained.

12.2.2 Transactions

317. 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.

318. Transaction documents must include:

- the name and address of the customer, underlying principal and beneficiary;
- 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.

319. 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

320. See section 7.4 of Chapter 7 for the record keeping requirements of wire transfer documents.

12.2.4 Internal and external suspicion reports

321. In order to meet the requirement to keep records of reports 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 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

322. 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

323. 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

324. 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 e.g. in civil court proceedings.

12.3.1 Ready retrieval

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

326. 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.

327. 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.

328. 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

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

330. When considering its policies, procedures and controls for the keeping of documents, a financial services business should weigh the needs of the investigating authorities against normal commercial considerations.

331. For example, when original vouchers are used for account entry, and are not

returned to the customer or agent, it is of assistance to the authorities if these original documents are kept for at least one year to assist forensic analysis (e.g. to investigate and prosecute cheque fraud).

12.5 Requirements on Closure or Transfer of Business

332. Where a financial services business terminates activities, or disposes of business or a block of business relationships, e.g. by way of asset sale, to another financial service provider the person taking on that business would be subject to the record keeping requirements in the Regulations.

PART 2 – SPECIFIC INDUSTRY SECTORS, APPENDICES AND GLOSSARY

CHAPTER 13 – SPECIFIC INDUSTRY SECTORS

Sections in this chapter

13. SPECIFIC INDUSTRY SECTORS

13.1 Banking

13.1.1 Scope of application

333. 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.

334. 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.

335. 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.

336. 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.

13.1.2 Suspicious features or activities

337. 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;
- 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;
- 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 securities 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.

13.1.3 Hold mail accounts

338. 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.

13.1.4 Bearer instruments

339. Certain countries or territories permit their companies to issue bearer shares 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 shares 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.

13.2 Fiduciary

13.2.1 Scope of application

340. 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.

13.2.2 Suspicious features or activities

341. 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.

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

343. 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.

13.3 Investment

13.3.1 Investment Funds

13.3.1.1 Scope of application

344. 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.

345. 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 4.8, 4.9 and 6.6 of the Handbook, rely on the intermediary or introducer to certify that they have verified the identity of the investor.

13.3.1.2 Suspicious features or activities

346. 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).

347. 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.

13.3.2 Discretionary and advisory asset management

13.3.2.1 Scope of application

348. 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.

13.3.2.2 Suspicious features or activities

349. Enhanced due diligence must be undertaken 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.

13.3.3 Intermediaries

350. The paragraphs below should be read together with section 6.6 of the Handbook.

13.3.3.1 Scope of application

351. 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.

352. "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.

13.3.3.2 Suspicious features or activities

353. 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.

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

355. 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.

13.4 Insurance

13.4.1 Scope of application

356. 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 must 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.

13.4.2 Suspicious features or activities

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

- The purchase of a significant single premium product, perhaps followed, in due course, by the early surrender or termination of the policy. Particular concern should be raised if this gives rise to a loss, or to a payment to a third party;
- Trusts and trustees, including both trusts within the ownership structure of a managed insurer, or premium payments to/from trusts in favour of those insured;
- 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 securities 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 remote, overseas countries or territories where comparable policies are available "closer to home";
- Transactions involving cash payments from third parties, or where settlement directions are for the benefit of 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.

358. Illustrations of the type of situation that might give rise to reasonable grounds for suspicion in certain 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.

CHAPTER 14 – APPENDICES

Appendices in this chapter

GUERNSEY STATUTORY INSTRUMENT
2007 No.

The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations, 2007

ARRANGEMENT OF REGULATIONS

GUERNSEY STATUTORY INSTRUMENT
2007 No.

The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations, 2007

Made	, 2007
Coming into operation	, 2007
Laid before the States	, 2007

THE POLICY COUNCIL, after consultation with the Guernsey Financial Services Commission and in exercise of the powers conferred upon it by section 49 of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 and 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) (Bailiwick of Guernsey) Regulations, 2007.

COMMENCEMENT

2. These Regulations shall come into force on the [ ], 2007.

RISK ASSESSMENT AND MITIGATION

3. (1) A financial services business must-

(a) carry out a suitable and sufficient business risk assessment-

(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;

(b) regularly review its business risk assessment 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;

(c) 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;

(d) regularly review any risk assessment carried out under subparagraph (c) so as

to keep it up to date and, where changes to that risk assessment are required, it must make those changes; and

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

(2) A financial services business must have regard to any relevant rules and guidance in the Handbook 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 which the financial services business knows, or has reasonable cause to suspect, is 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) any customer shall be identified and his identity verified using identification data;

(b) any introducer or other 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) any 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 identity 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 where the customer is established or situated in a country or territory -

(i) that does not apply or insufficiently applies the Financial Action Task Force Recommendations on Money Laundering; or

(ii) in respect of which the Commission considers there to be a high risk; and

(d) a business relationship or an occasional transaction which has been assessed as a high risk relationship pursuant to regulation 3(1)(c).

(2) In paragraph (1) -

(a) "enhanced customer due diligence" means additional steps in relation to identification and verification to those required under regulation 4(3) including taking the following steps -

(i) considering whether additional identification data needs to be obtained;

(ii) considering whether additional aspects of the customer's identity need to be verified;

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

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

(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) Where a business relationship falls within paragraph (1)(a), a financial services business must ensure that senior management approval is obtained for establishing, or, in the case of an existing business relationship, continuing that relationship.

(4) Where the customer was not physically present 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(1)(c), 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 -

(a) in accordance with the requirements set out in Chapter 6 of the Handbook;

and

(b) provided that the customer and every beneficial owner and underlying principal is established or situated in the Bailiwick or a country or territory listed in Appendix C to the Handbook.

(3) For the avoidance of doubt, simplified or reduced customer due diligence shall not be applied -

(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) Identification of the beneficiaries of a trust or other legal arrangement and verification of the identity of customers 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 names which it knows, or has reasonable cause to suspect, to be fictitious; 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, to ensure compliance with the Financial Action Task Force Recommendations on Money Laundering and other international requirements, in relation to all aspects of a banking group's business carried on worldwide and in accordance with the Core Principles of Effective Banking Supervision issued by the Basel Committee on Banking Supervision;

(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 unafilliated with a banking group which is subject to effective consolidated supervision.

NON-COMPLIANCE WITH CUSTOMER DUE DILIGENCE MEASURES ETC.

9. (1) Where a financial services business can not comply with any of regulation 4(3)(a) to (d) it must, subject to paragraph (2) -

(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 report must be made pursuant to regulation 12(c).

(2) Where this regulation applies in the circumstances set out in regulation 4(2)(c), the business relationship or occasional transaction may be entered into or carried out in accordance with directions given by a police officer duly authorised for that purpose.

INTRODUCED BUSINESS

10. (1) In the circumstances set out in paragraph (2), a financial services business may accept a written confirmation of identity 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, subject to limited exceptions provided for in Chapter 4 of the Handbook, keeps such identification data and documents.

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

(a) is an Appendix C financial services business; or

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

(i) the head office of both the introducer and the receiving financial services business fall within paragraph (2)(a); and

(ii) the introducer -

(A) where it is an overseas branch, is subject to effective policies, procedures and controls on countering money laundering and terrorist financing of the receiving financial services business; or

(B) where it is a member of the same group of companies, is subject to effective policies, procedures and controls on countering money laundering and terrorist financing of a common parent company to which the receiving financial services business is also subject.

(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) on going customer due diligence which shall include 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 a police officer 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 effective and appropriate procedures and controls as are necessary to ensure compliance with 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 effective and appropriate 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; and

(c) the implications of non-compliance by employees with any rules or guidance 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) Documents (including copies) and customer due diligence information 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 to any police officer, the Commission or any other person where such documents or customer due diligence information are requested pursuant to these Regulations or any relevant enactment.

(3) 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 or customer due diligence information so provided.

(4) A financial services business shall also keep records of -

(a) any reports made to a money laundering reporting officer under regulation 12 for five years starting from -

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

(ii) in the case of a report 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.

ENSURING COMPLIANCE, CORPORATE RESPONSIBILITY AND RELATED REQUIREMENTS

15. 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) 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,

to the extent that the law of that country or territory allows and if the law of any country or territory does not so allow in relation to any requirement of the Regulations, the financial services business must notify the Commission accordingly.

PART IV
MISCELLANEOUS

MONEY OR VALUE TRANSMISSION SERVICES-LISTS OF AGENTS.

16. Any person which 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

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) Where an offence under paragraph (1) committed by a body corporate is proved to have been committed with the consent or connivance, or to be attributable to any

neglect on the part of, any director, manager, secretary or other similar officer of the body corporate or any person who is purporting to act in any such capacity he, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

(3) Where the affairs of a body corporate are managed by the members, paragraph (2) 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 of a body corporate.

(4) Where an offence under paragraph (1) committed by a partnership, or by an unincorporated association other than a partnership, is proved to have been committed with the consent or connivance of, or is attributable to any neglect on the part of, any partner in the partnership or (as the case may be) a person concerned in the management or control of the association, he, as well as the partnership or association, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

AMENDMENT TO THE LAW

18. (1) The Law shall be amended as follows.

(2) For the Schedule to the Law substitute the Schedule 1 set out in the Schedule to these Regulations.

DEFINITIONS

19. (1) In these Regulations, unless the context otherwise requires -

"account" means a bank account and any other similar business relationship between a financial services business and a customer;

"appendix C financial services business" means -

(a) a financial services business supervised by the Commission; or

(b) a business -

(i) which is carried on from 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;

(ii) 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;

(iii) 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

(iv) the conduct of which is supervised for compliance with the requirements

referred to in subparagraph (iii), by 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 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

(b) a person on whose behalf the business relationship or occasional transaction is being conducted and, in the case of a trust or other legal arrangement, this shall mean -

(i) any beneficiary in whom an interest has vested; and

(ii) any other person who appears likely to benefit from that 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 continuing arrangement between the financial services business in question and another party, to facilitate the carrying out of transactions, in the course of such financial service business -

(a) on a frequent, habitual, or regular basis; and

(b) where the monetary value of any transactions to be carried out in the course of the arrangement is not known on entering into the arrangement;

"business risk assessment" means an assessment which documents the exposure of a business to risks 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;

"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 form, or has formed, 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 enters into the business relationship;

"customer document" means a document obtained or created by a financial services business in order to satisfy itself as to the identity of the customer or any beneficial owner or underlying principal;

"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;

"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);

"Financial Action Task Force Recommendations on Money Laundering" includes the Financial Action Task Force Special Recommendations on Terrorist

Financing;

"financial services business" means any business specified in Schedule 1 to the Law;

"Handbook" means the Handbook on Countering Financial Crime and Terrorist Financing as revised or re-issued from time to time by the Commission;

"high risk relationship" means a business relationship or an occasional transaction which has a high risk of involving money laundering or terrorist financing and related terms shall be construed accordingly;

"identification data" means data, documents or information, in any form whatsoever, which is from a reliable and independent source;

"intermediary" means an introducer which meets the criteria for it to be treated as a customer set out in Chapter 6 of the Handbook;

"introducer" means a financial services business which enters, on behalf of another person or legal arrangement who is its customer, into a business relationship with another 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, a period of five years starting from the date-

    (i) where the customer has formed a business relationship with the financial services business, that relationship ceased;

    (ii) where the customer has carried out an occasional transaction with the financial services business, that transaction was completed,

    or such other period as the Commission may direct;

(b) in the case of a transaction document, a period of five years starting from the date that both the transaction and any related transaction were completed or such other 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;

(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

(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 in several operations that appear to be linked;

"ongoing customer due diligence" shall be construed in accordance with regulation 11(1)(c);

" police officer" has the meaning in section 51(1) of the Law;

"politically exposed person" shall be construed in accordance with regulation 5(2);

"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) the Money Laundering (Disclosure of Information) (Guernsey) Law, 1995;

(b) the Money Laundering (Disclosure of Information) (Alderney) Law, 1998;

(c) the Law;

(d) the Drug Trafficking (Bailiwick of Guernsey) Law, 2000;

(e) the Money Laundering (Disclosure of Information) (Sark) Law, 2001;

(f) the Terrorism (United Nations Measures) (Channel Islands) Order 2001;

(g) the Al-Qaida and Taliban (United Nations Measures) (Channel Islands) Order 2002;

(h) the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002;

(i) the Transfer of Funds (Guernsey) Ordinance, 2007;

(j) the Transfer of Funds (Alderney) Ordinance, 2007;

(k) the Transfer of Funds (Sark) Ordinance, 2007;

(l) the Disclosure (Bailiwick of Guernsey) Law, 2007,

and such laws 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 conduct which constitutes an offence under any of sections 8 to 11 of the Terrorism Law and, for the purposes of this definition, the "purposes of terrorism" shall include, to the extent that they do not already do so -

(a) any attempt, conspiracy or incitement to carry out terrorism within the meaning of section 1 of the Terrorism Law; or

(b) aiding, abetting, counselling or procuring the carrying out of such terrorism;

"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 or a protector of a trust which is the customer or the beneficiaries of which are the beneficial owners; or

(b) exercises ultimate effective control over the customer or 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.

(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 applies to the interpretation of these Regulations.

REVOCATION

20. The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations, 2002 are hereby revoked.

Dated this day of , 2007

Chief Minister
For and on behalf of the Policy Council

SCHEDULE

regulation 18

AMENDMENT TO THE LAW

"SCHEDULE 1

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 19 are only financial services businesses when carried on by way of business.

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.

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).

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.

7. Providing financial guarantees or commitments.

8. Trading for account of customers (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, including, without limitation, bullion.

9. Participating in securities 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.

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.

19. The provision of services in relation to any of the financial services businesses falling within paragraphs 2 to 18.

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 "insurance business" as defined in the Insurance Business (Bailiwick of Guernsey) Law, 2002, or doing anything -

    (a) which can only lawfully be done under the authority of a licence of the Commission under the Insurance Managers and Insurance Intermediaries (Bailiwick of Guernsey) Law, 2002; or

    (b) the doing of which is specifically exempted by that Law from the requirement to hold such a licence;

23. Carrying on "regulated activities" as defined in the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc. (Bailiwick of Guernsey) Law, 2000.

PART II
INCIDENTAL AND OTHER ACTIVITIES

24. (1) Any financial services business falling within paragraphs 2 to 19 carried out in the course of carrying on the profession of -

(a) a lawyer where such business is incidental to the provision of legal advice or services;

(b) an accountant where such business is incidental to the provision of accountancy advice or services;

(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 financial services business falling within paragraphs 2 to 19; 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 financial service business -

(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. Any financial services business falling within any of paragraphs 2, 3, 7, 9 and 11 or falling within paragraph 19 by virtue of it being a service carried out in relation to any such business described in those paragraphs where that business is only carried on by a body corporate ("first company") in the course of providing services to another body corporate -

(a) of which the first company is the sole shareholder;

(b) which is the first company's sole shareholder; or

(c) which has the same sole shareholder as the first company.".

APPENDIX B

GUIDANCE ON CORPORATE GOVERNANCE IN THE FINANCE SECTOR IN GUERNSEY

INTRODUCTION

This paper has been produced in response to requests from the finance sector to provide guidance on the Commission's corporate governance expectations as they apply to all financial services businesses. It outlines what the Commission considers to be basic requirements for a sound corporate governance regime for the finance sector in Guernsey and details those areas that every Director[1] and manager of a finance business is expected to consider. This paper is not intended to be prescriptive, but is intended to provide direction and principles from which an approach to corporate governance appropriate to the circumstances of an individual organisation can be developed and implemented. An organisation's approach to corporate governance will reflect ownership, legal and operating structures.

The guidance applies to all regulated financial services businesses in the Bailiwick of Guernsey and failure to meet these basic standards will be taken into consideration by the Commission in determining whether licensees or individuals are fit and proper. It should be taken to apply as follows to each specific sector:-

- Section 36C of the Banking Supervision (Bailiwick of Guernsey) Law, 1994 requires banks, inter alia, to review, not less than once every financial year, whether they have in place control systems which are effective to ensure the responsibilities and conduct of the bank's Board of Directors with respect to corporate governance principles. This guidance provides advice on what the Commission sees as banks' responsibilities and their Boards' expected conduct with respect to corporate governance principles.
- Businesses holding full fiduciary licences should consider this guidance in relation to their compliance with legal obligations such as the "four eyes" criterion and the relevant provisions of the Codes of Practice for Corporate Services Providers, Trust Service Providers and Company Directors issued under section 35 of the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc. (Bailiwick of Guernsey) Law, 2000.
- Licensed insurers will meet the standards laid out in this guidance if they comply with their obligations under the Licensed Insurers' Corporate Governance Code of 4 July 2003 issued under the provisions of section 78 of the Insurance Business (Bailiwick of Guernsey) Law, 2002.
- Businesses holding insurance managers' licences and/or intermediary licences should consider this guidance in relation to their compliance with Schedule 4 to the Insurance Managers and Insurance Intermediaries (Bailiwick of Guernsey) Law, 2002 and with the relevant provisions of the Codes and Regulations issued under that law.
- Firms licensed under the Protection of Investors (Bailiwick of Guernsey) Law, 1987 should consider this guidance in relation to their compliance with the relevant provisions of Part 4 of the Licensees (Financial Resources, Notification, Conduct of Business and Compliance) Rules 1998.

---

[1]In the case of partnerships, the term "director" in this paper also applies to partners and the term "Board of Directors" applies to the partners.

Corporate governance refers to all those measures required to effectively oversee the direction and management of organisations and encompasses setting, controlling, monitoring and reviewing strategy, objectives, corporate values, risk management, delegation of responsibility and accountability, transparency and ethical behaviour.

The effectiveness of the approach to corporate governance by directors and management has a critical influence on each firm's, and as a consequence on the finance sector's, viability. Good corporate governance practice improves safety and soundness through effective risk management and creates the ability to execute strategy and achieve business objectives in a manner that promotes confidence and protects the interest of stakeholders. The nature of a stakeholder will vary according to the type of financial services business but could include, for example, shareholders, depositors, policyholders, employees, creditors and clients.

GUIDANCE ON CORPORATE GOVERNANCE IN THE FINANCE SECTOR IN GUERNSEY

General Responsibilities of the Board of Directors

The Board of Directors ("the Board") is responsible for the corporate governance of the organisation. Members of the Board should be proactive in recognising and understanding the risks the organisation faces in achieving its business objectives and should demonstrate effective and prudent management of those risks.

The Board should ensure that the organisation's operations are conducted reasonably and within the framework of any applicable laws, regulations, rules, guidelines and codes as well as established policies and procedures.

Risk Management

The Board and management should analyse existing and prospective business, products and services to identify and measure the types and significance of the current and potential risks to be managed and controlled, both individually and in the aggregate. The Board and management should develop and implement appropriate and prudent risk management policies and procedures and monitor their effectiveness through timely, accurate and complete information systems.

Internal Control Procedures

The Board should establish internal control procedures that are, in the Board's opinion, necessary and sufficient for the purposes of managing operational risks and conducting the organisation's business having regard to its size, nature and complexity.

Duties of Directors

The Board should ensure that collectively its members have sufficient expertise to understand and challenge the important issues in relation to the operation and control of the organisation.

Each Director, in exercising the powers of a Director and discharging the duties as a Director, should act with honesty, integrity and in good faith with a view to the best interests of the organisation and its stakeholders.

Composition of the Board of Directors

The Board should regularly review its composition, taking into account the nature, scale and complexity of the business, and the requirements of any applicable laws, regulations, rules, guidelines and codes.

Self Assessment

The Board should regularly assess and document whether its approach to corporate governance achieves its objectives and, consequently, whether the Board itself is fulfilling its own responsibilities. The Board should review the effectiveness of its overall approach to governance and make changes where that effectiveness needs to be enhanced. In carrying out this review the Board should assess whether the organisation's control environment is appropriate and effective, taking into account the nature and scale of the business, its approach to governance, management and style of communication, organisation structure, resource availability, procedures and controls.

Guernsey Financial Services Commission
10 December 2004

APPENDIX C

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

Austria
Australia
Belgium
Canada
Denmark
Finland
France
Germany
Gibraltar
Greece
Hong Kong
Iceland
Ireland
Isle of Man
Italy
Japan
Jersey
Luxembourg
Netherlands
New Zealand
Norway
Portugal
Singapore
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.

Bailiwick of 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. Bailiwick of 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 "**appendix C financial services business**" means -

(a) a financial services business supervised by the Commission; or

(b) a business -

(i) which is carried on from 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;

(ii) 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;

(iii) 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

(iv) the conduct of which is supervised for compliance with the requirements referred to in subparagraph (c), by an overseas regulatory authority.

The absence of a country or territory from the above list does not prevent the application of section 4.8.1 of the Handbook (reliable introductions by an overseas branch or member of the same group, subject to satisfactory terms of business).

SENSITIVE JURISDICTIONS

From time to time the Commission issues Business From Sensitive Sources Notices. Transactions to or from the jurisdictions specified in such Notices must be subject to a greater level of caution and scrutiny.

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*			

** The 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

Name and address of financial services business		
Sort code		
STRICTLY PRIVATE AND CONFIDENTIAL		
Your ref:	Our ref:	Date:

The Financial Intelligence Service, Hospital Lane, St Peter Port, Guernsey, GY1 2QN
Tel: 714081 Fax: 710466 E-mail: director@guernseyfis.org

Legislation under which this disclosure is made *(please tick one of the following)*:

Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 ☐
Discloure (Bailiwick of Guernsey) Law, 2007 ☐

Subject's full name(s)			
Date(s) of birth			
Passport or ID number			
Nationality			
Address(es)			
Telephone	Home:	Work:	Mobile:
Occupation/employer			
Associated company: *e.g. company registration number, date and place of incorporation, etc.*			
Account/product number			
Date account/product opened			
Details of any intermediary			
Other relevant information: *e.g. additional details of identification and/or references taken, associated parties, addresses, telephone numbers, etc.)*			

DISCLOSURE (CONTINUED)

Reasons for suspicion:	
Current status of business relationship:	
Contact name	
Telephone number	
Signed	

When submitting this report, please append any additional material that you may consider relevant and which may be of assistance to the recipient, i.e. bank statements, vouchers, international transfers, inter-account transfers, telegraphic transfers, details of associated accounts and products, etc.

APPENDIX D3

SPECIMEN ACKNOWLEDGEMENT OF THE FIS

MLRO Your Ref:

PRIVATE & CONFIDENTIAL - ADDRESSEE ONLY

Dear

Thank you for the disclosure of information you have provided under the provisions of Section 39 of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended concerning:-

XXXXXX XXXXXXX

Your suspicions have been noted.

Thank you for your continued co-operation.

Yours sincerely

APPENDIX D4

SPECIMEN CONSENT OF THE FIS

MLRO Your Ref:

PRIVATE & CONFIDENTIAL - ADDRESSEE ONLY

Dear

Thank you for the disclosure of information you have provided under the provisions of Section 39 of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended concerning:-

XXXXXX XXXXXXX

Your suspicions have been noted.

Based upon the information provided you have consent to

However, this consent 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 the subject.

Thank you for your continued co-operation.

Yours sincerely

Please note that it is proposed to make separate Ordinances in respect of Guernsey, Alderney and Sark. Only one draft Ordinance (see below) has been prepared to date – separate Ordinances will only be drafted when the contents of this single Ordinance have been finalised. As a result, the references to Guernsey/Alderney/Sark in this Ordinance, for example in the heading below, will be amended so that each individual Ordinance is only applicable to Guernsey/Alderney/Sark as appropriate.

The Transfer of Funds (Guernsey/Alderney/Sark) Ordinance, 2007

ARRANGEMENT OF SECTIONS

PART I

INFORMATION TO ACCOMPANY TRANSFERS OF FUNDS

PART II

ENFORCEMENT

PART III

GENERAL

The Transfer of Funds (Guernsey/Alderney/Sark) Ordinance, 2007

THE STATES, in pursuance of their Resolution of the 28th day of September 2005 , and in exercise of the powers conferred upon them by sections 1 and 4 of the European Communities (Implementation) (Bailiwick of Guernsey) Law, 1994 and of all other powers enabling them in that behalf, hereby order:-

PART I
INFORMATION TO ACCOMPANY TRANSFERS OF FUNDS

Application.

1. (1) Subject to subsection (2), this Ordinance applies in relation to transfers of funds in any currency which are sent or received by a payment service provider established in Guernsey/Alderney/Sark.

(2) This Ordinance shall not apply to the transfers of funds set out in the Schedule.

Information accompanying transfers of funds and record keeping.

2. (1) Subject to sections 3, 4(1) and 9 a payment service provider must ensure that transfers of funds are accompanied by complete information on the payer as set out in subsection (2).

(2) Complete information on the payer shall consist of the name, address and account number of the payer except that -

(a) the address of the payer may be substituted with his date and place of birth (where relevant), his customer identification number or national identity number, and

(b) where the payer does not have an account number, the payment service provider of the payer shall substitute it with a unique identifier, which allows the transaction in question to be traced back to that payer.

(3) Subject to the following provisions of this section, the payment service provider of the payer must, before transferring any funds, verify the complete information on the payer and such verification must be on the basis of documents, data or other information obtained from a reliable and independent source.

(4) In the case of transfers of funds from an account, the payment service provider of the payer may deem verification to have taken place if -

(a) a payer's identity has been verified in connection with the opening of that account and the information obtained by that verification has been retained in accordance with regulations 4 to 6 and 14 of the 2007 Regulations , or

(b) the payer is an existing customer and it is appropriate to do so taking into account the risk of money laundering or terrorist financing occurring.

(5) Except where verification of the payer must be carried out in accordance with regulations 4 to 6 of the 2007 Regulations, where a transfer of funds is not made from an account, the payment service provider of the payer must verify the information on the payer only where –

(a) the amount transferred exceeds 1000 Euros, or

(b) the transaction is carried out in one of several operations -

(i) that appear to the payment service provider of the payer to be linked, and

(ii) which together exceed 1000 Euros.

(6) The payment service provider of the payer shall keep records of the complete information on the payer for five years from the date of the transfer of funds in question in accordance with regulation 14 of the 2007 Regulations.

Transfers of funds within the British Islands.

3. (1) Subject to subsection (2), where both the payment service provider of the payer and the payment service provider of the payee are situated in the British Islands, a transfer of funds need only be accompanied by -

(a) the account number of the payer, or

(b) where there is no such account number, a unique identifier which allows the transaction in question to be traced back to the payer.

(2) The payment service provider of the payer shall make available to the payment service provider of the payee complete information on the payer within 3 working days of its receipt of a request for such information from the payment service provider of the payee.

Transfers of funds from the British Islands to outside the British Islands.

4. Where there is a batch file transfer from a single payer where some or all of the payment service providers of the payees are situated outside the British Islands, section 2(1) shall not apply to each of the individual transfers of funds which are bundled together for transmission, provided that -

(a) the batch file contains the complete information on the payer in question, and

(b) each of the individual transfers carries the account number of the payer or a unique identifier.

Detection of missing information on the payer.

5. A payment service provider of a payee must -

(a) in the messaging or payment and settlement system used to effect a transfer of

funds, detect whether the fields relating to information on the payer have been completed using the characters or inputs admissible within the conventions of that messaging or payment and settlement system,

(b) have effective procedures in place to detect whether the following information on the payer is missing -

(i) for transfers of funds where the payment service provider of the payer is situated in the British Islands, the information required under section 3, and

(ii) subject to subparagraph (iii), for transfers of funds where the payment service provider of the payer is situated outside the British Islands-

(A) complete information on the payer, or

(B) where relevant, the information required under section 9, and

(iii) for batch file transfers where the payment service provider is situated outside the British Islands, the information on the payer required by section 4.

Transfers of funds with missing or incomplete information on the payer.

6. (1) If a payment service provider of a payee becomes aware, when receiving transfers of funds, that information on the payer required under this Ordinance, is missing or incomplete then, it must, subject to subsections (2) and (3)-

(a) reject the transfer,

(b) request from the payment service provider of the payer the complete information on the payer, or

(c) take such other steps as the Commission may by order direct.

(2) Notwithstanding the requirement in subsection (1), the payment service provider of the payee must comply with any relevant requirements of any other enactment relating to money laundering or terrorist financing.

(3) The payment service provider of the payee in deciding whether or not to reject the transfer or request complete information must take into account any relevant guidance issued by the Commission.

(4) Where a payment service provider of a payer regularly fails to supply information on the payer required under this Ordinance, the payment service provider of the payee must –

(a) notify the Commission and a police officer of that fact, and

(b) take steps to attempt to ensure that such information is supplied and such steps may initially include the issuing of written warnings and written deadlines regarding the supply of the required information.

(5) If, following the taking of steps under subsection (4), a payment service provider of a payer still regularly fails to supply the required information on the payer, the payment service provider of the payee must –

(a) reject any future transfers of funds from that payment service provider, or

(b) decide whether or not to restrict or terminate its business relationship with that payment service provider.

Risk-based assessment and record keeping.

7. (1) Where information on the payer accompanying a transfer of funds is missing or incomplete, the payment service provider of the payee must take this into account in assessing whether the transfer of funds, or any related transaction, is suspicious, and whether -

(a) a failure to disclose its suspicion as soon as reasonably practicable would be an offence under section 1(1) or 2(1) of the Disclosure Law, and

(b) a failure to disclose its suspicion as soon as reasonably practicable would be an offence under section 15 [or 15A] of the Terrorism Law.

(2) The payment service provider of the payee shall keep records of any information received by it on the payer for five years from the date of the transfer of funds in question.

Keeping information on the payer with the transfer.

8. Subject to section 9, any intermediary payment service provider must ensure that any information received by it on the payer that accompanies a transfer of funds is kept with that transfer.

Technical limitations.

9. (1) This section applies where a payment service provider of a payer is situated outside the British Islands and the intermediary payment service provider is situated within the British Islands.

(2) An intermediary payment service provider may use a payment system with technical limitations to send a transfer of funds to a payment service provider of a payee except that where it is aware that information on the payer which is required under this Ordinance is missing or incomplete it must comply with subsection (3).

(3) Where an intermediary payment service provider becomes aware, when receiving a transfer of funds, that information on the payer required under this Ordinance is missing or incomplete, it may only use a payment system with technical limitations

if –

(a) it notifies the payment service provider of the payee that the information is missing or incomplete through–

(i) a payment or messaging system, or

(ii) another procedure, and

(b) the system or procedure is agreed between the intermediary payment service provider and the payment service provider of the payee.

(4) Where an intermediary payment service provider uses a system with technical limitations, it shall, upon request from the payment service provider of the payee, make available to the payment service provider of the payee, all information on the payer which it has received, within 3 working days excluding the day on which the request was received.

(5) An intermediary payment service provider must keep records of any information on the payer received by it in respect of transfers falling within subsections (2) and (3) for five years from the date of the transfer in question.

(6) In this section "technical limitations" means technical limitations which prevent information on the payer accompanying transfers of funds.

Cooperation obligations.

10. (1) Payment service providers shall comply fully and without delay with -

(a) any requirement or warrant to provide information or documents pursuant to section 25, 26, 28 or 29 of the Banking Law, 1994 as applied by section 11,

(b) any requirement to provide information or documents, however expressed, under -

(i) the Drug Trafficking (Bailiwick of Guernsey) Law, 2000 ,

(ii) the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 ,

(iii) the Terrorism Law,

(iv) the 2007 Regulations,

(v) the Terrorism (United Nations Measures) (Channel Islands) Order 2001 , or

(vi) the Al-Qa'ida and Taliban (United Nations Measures) (Channel Islands) Order 2002 ,

where such information or documents comprises information on the payer which accompanies any transfer of funds or corresponding records.

(2) Subject to any other enactment, any information or documents to which subsection (1) applies may only be used for the purposes of preventing, investigating, or detecting money laundering or terrorist financing.

PART II
ENFORCEMENT

Monitoring and enforcement-information seeking powers.

11. (1) The provisions of sections 25 (power to obtain information and documents) and 26 (right of entry to obtain information and documents) of the Banking Law shall apply –

(a) to payment service providers who send or receive transfers of funds to which this Ordinance applies as they apply to licensed institutions within the meaning of that Law,

(b) in relation to such information as the Commission may reasonably require for the purpose of effectively monitoring or ensuring compliance with the requirements of this Ordinance as they apply in relation to such information as the Commission may reasonably require for the performance of its functions under that Law, and

(c) as if section 25(11) of that Law also allowed the powers referred to in that section to be exercised if the Commission considers that it is desirable to do so in the interests of effectively monitoring or ensuring compliance with the requirements of this Ordinance,

except that section 25(10) (information required for determining whether person is a fit and proper person) of that Law shall not apply.

(2) Sections 28 (investigation of suspected offences) and 29 (power of entry in cases of suspected offences) of the Banking Law shall apply in relation to an offence under this Ordinance as they apply in relation to an offence under section 1 or 21 of that Law.

(3) Section 44 (cases where disclosure is permitted) of the Banking Law shall apply as if it also permitted the disclosure of information in compliance with, or for the purposes of enabling or assisting a person to comply with, any requirement of this Ordinance.

(4) References in any enactment to section 25, 26, 28 or 29 of the Banking Law shall be construed as including references to those sections as applied by this section.

Offences.

12. (1) Any payment service provider who, without reasonable excuse, fails to comply

with any of the requirements of sections 2 to 11 of this Ordinance shall be guilty of an offence and on -

(a) summary conviction be liable to imprisonment for a term not exceeding 6 months or to a fine not exceeding level 5 on the uniform scale, or both, and

(b) conviction on indictment be liable to imprisonment for a term not exceeding five years, a fine, or both.

Criminal proceedings against unincorporated bodies.

13. (1) Where an offence under this Ordinance is alleged to have been committed by an unincorporated body, proceedings for the offence shall be brought in the name of that body and not in the name of any of its members.

(2) A fine imposed on an unincorporated body on its conviction for an offence under this Ordinance shall be paid from the funds of that body.

(3) Where an offence under this Ordinance is committed by an unincorporated body and is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of -

(a) any director thereof or any other officer thereof who is bound to fulfil any duty whereof the offence is a breach,

(b) any partner thereof (in the case of a partnership), or

(c) any person purporting to act in any capacity described in paragraph (a) or (b),

he as well as the unincorporated body is guilty of the offence and may be proceeded against and punished accordingly.

Criminal liability of directors, etc.

14. (1) Where an offence under this Ordinance is committed by a company 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, chief executive, controller, manager, secretary or other similar officer of the company or any person purporting to act in any such capacity, he as well as the company is guilty of the offence and may be proceeded against and punished accordingly.

(2) Where the affairs of a company are managed by its members, subsection (1) applies to a member in connection with his functions of management as if he were a director.

PART III
GENERAL

Power for Commission to make rules, instructions and guidance.

15. (1) The Commission may make rules, instructions and guidance for the purposes of

this Ordinance.

(2) Any court shall take the rules, instructions and guidance into account in determining whether or not any person has complied with the Ordinance.

Regulations, orders, rules, instructions and guidance.

16. (1) Any provision of this Ordinance may be amended by Regulations made by the [.]

(2) Any Regulations, order, rules, instructions or guidance under this Ordinance -

(a) may be amended or repealed by subsequent Regulations, an order, rules, instructions or guidance, as the case may be,

(b) may contain consequential, incidental, supplemental and transitional provisions, and

(c) in the case of Regulations or an order, shall be laid before a meeting of the States as soon as possible and shall, if at that or the next meeting the States resolve to annul them, cease to have effect, but without prejudice to anything done under them or to the making of new Regulations.

(3) Any power conferred by this Ordinance to make Regulations, an order, rules, instructions or guidance may be exercised -

(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, and

(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, and

(iii) any such provision either unconditionally or subject to any conditions specified in the Regulations, order, rules, instructions or guidance.

Interpretation.

17. (1) In this Ordinance, unless the context otherwise requires -

"2007 Regulations" means the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Regulations, 2007,

"Banking Law" means the Banking Supervision (Bailiwick of Guernsey) Law, 1994,

"batch file transfer" means several individual transfers of funds which are bundled together for transmission,

"British Islands" means the United Kingdom, the Channel Islands and the Isle of Man,

"Commission" means the Guernsey Financial Services Commission established by the Financial Services Commission (Bailiwick of Guernsey) Law, 1987 ,

"complete information" shall be construed in accordance with section 2(2),

"Department of the States" includes any council or committee (however called) thereof,

"Disclosure Law" means the Disclosure (Bailiwick of Guernsey) Law, 2007,

"document" includes information recorded in any form (including, without limitation, in electronic form),

"EC Regulation" means Regulation (EC) No. 1781/2006 of the European Parliament and of the Council of the 15th November 2006 on information on the payer accompanying transfers of funds ,

"electronic money" means monetary value as represented by a claim on the issuer which is –

(a) stored on an electronic device,

(b) issued on receipt of funds of an amount not less in value than the monetary value issued, and

(c) accepted as means of payment by persons other than the issuer,

"enactment" includes a Law, an Ordinance or any subordinate legislation and any provision or portion of a Law, an Ordinance or any subordinate legislation,

"intermediary payment service provider" means a payment service provider, neither of the payer nor of the payee, that participates in the execution of transfers of funds,

"money laundering" is any act which –

(a) constitutes an offence under section 38, 39 or 40 of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999,

(b) constitutes an offence under section 57, 58 or 59 of the Drug Trafficking (Bailiwick of Guernsey) Law, 2000,

(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 such an offence if done in the Bailiwick of Guernsey,

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,

"notify" means notify in writing,

"payee" means a person who is the intended final recipient of transferred funds,

"payer" means -

(a) a person who holds an account and allows a transfer of funds from that account, or

(b) where there is no account, a person who places an order for a transfer of funds,

"payment service provider" means a person whose business includes the provision of transfer of funds services,

"person" includes body or authority,

"police officer" means -

(a) a member of the salaried police force of the Island of Guernsey/Alderney/Sark and, within the limits of his jurisdiction, a member of the special constabulary of the Island of Guernsey/Alderney/Sark, and

(b) an officer within the meaning of section 1(1) of the Customs and Excise (General Provisions) (Bailiwick of Guernsey) Law, 1972 ,

"States" means the States of Guernsey/Alderney/Sark,

"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 conduct which constitutes an offence under any of sections 8 to 11 of the Terrorism Law and, for the purposes of this definition, in those sections the "purposes of terrorism" shall, include, to the extent that they do not already do so -

(a) any attempt, conspiracy or incitement to carry out terrorism within the meaning of section 1 of the Terrorism Law, or

(b) aiding, abetting, counselling or procuring the carrying out of such terrorism,

"transfer of funds" means any transaction carried out on behalf of a payer through a payment service provider by electronic means, with a view to making funds available to a payee at a payment service provider, irrespective of whether the payer and the payee are the same person,

"uniform scale of fines" means the uniform scale of fines from time to time in force under the Uniform Scale of Fines (Bailiwick of Guernsey) Law, 1987 ,

"unique identifier" means a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement or messaging system used to effect the transfer of funds,

and any other terms which are used in this Ordinance and which are also used in the EC Regulation shall have the same meaning as in the EC Regulation.

(2) For the purposes of this Ordinance references to Euros shall be converted to pounds sterling or any other relevant currency at the relevant rate of conversion from time to time published in the "C" Series of the Official Journal of the European Communities.

(3) In this Ordinance, words importing the neutral gender include the feminine and masculine gender and vice versa.

(4) Any reference in this Ordinance to an enactment or to European Community legislation is a reference thereto as from time to time amended, re-enacted (with or without modification), extended or applied.

Extent.

18. This Ordinance has effect in the islands of Guernsey, Herm and Jethou/Alderney/Sark.

Citation.

19. This Ordinance may be cited as the Transfer of Funds (Guernsey/Alderney/Sark) Ordinance, 2007.

Commencement.

20. This Ordinance shall come into force on the [, 2007.]

SCHEDULE
TRANSFERS OF FUNDS TO WHICH ORDINANCE DOES NOT APPLY

1. A transfer of funds carried out using a credit or debit card provided that -

   (a) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services, and

   (b) a unique identifier, which allows the transaction to be traced back to the payer, accompanies such transfer.

2. A transfer of funds carried out using electronic money where the transfer does not exceed 1,000 Euros and if the device on which the electronic money is stored –

   (a) cannot be recharged, the maximum amount stored in the device is 150 Euros, or

   (b) can be recharged, a limit of 2,500 Euros is imposed on the total amount transacted in a calendar year unless an amount of 1,000 Euros or more is redeemed in that same calendar year by the bearer of the device.

3. Without prejudice to paragraph 2, a transfer of funds carried out by means of a mobile telephone or any other digital or information technology device, provided that the transfer –

   (a) is pre-paid, and

   (b) does not exceed 150 Euros.

4. A transfer of funds carried out by means of a mobile telephone or any other digital or information technology device provided that –

   (a) the transfer is post-paid,

   (b) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services,

   (c) a unique identifier, allowing the transaction to be traced back to the payer, accompanies the transfer, and
   (d) the payment service provider is subject to the obligations set out in section 1 of the Disclosure Law, section 15 of the Terrorism Law and the 2007 Regulations or to similar obligations under the law of any part of the British Islands.

5. A transfer of funds –

   (a) where the payer withdraws cash from his own account,

(b) where there is authorisation for a debit transfer between two persons which permits payments between them through accounts, provided that a unique identifier accompanies the transfer of funds, which enables the transaction to be traced back to the payer,

(c) where truncated cheques are used,

(d) within the British Islands, to any public authorities, including any Department of the States or Parochial officers, in respect of any taxes, rates, fines or any other levies whatsoever, or

(e) where both the payer and the payee are payment service providers acting on their own behalf.

APPENDIX F

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 on the Countering of Financial Crime and the Financing of Terrorism ("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 ☐

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

(if a Company or Partnership): Date and place of incorporation and registration number		Are bearer shares currently in issue? Yes ☐ No ☐
(if a Company or Partnership): Current registered office address		If no, can bearer shares be issued? Yes ☐ No ☐
(if a Trust or Foundation): Date of establishment and legal jurisdiction		
Type of trust/foundation/company		Is it a trading company? 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):	
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		

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		

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		

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 and 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 a 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, e.g. "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 bank/deposit taker or accepting financial services business should you have any doubt or queries about completing the Introducer Certificate Forms.

APPENDIX G

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 financial services business and in respect of this account it has obtained and holds the verification required to satisfy the Handbook on the Countering of Financial Crime and the Financing of Terrorism ("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 ☐

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

(if a Company or Partnership): Date and place of incorporation and registration number		Are bearer shares currently in issue? Yes ☐ No ☐
(if a Company or Partnership): Current registered office address		If no, can bearer shares be issued? Yes ☐ No ☐
(if a Trust or Foundation): Date of establishment and legal jurisdiction		
Type of trust/foundation/company		Is it a trading company? 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)	
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		

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		

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 ☐ ☐

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 financial services 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 a 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, e.g. "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 H

LINKS TO USEFUL WEBSITE ADDRESSES

APPENDIX I

EXAMPLES OF MONEY LAUNDERING AND TERRORIST FINANCING

APPENDIX J

GLOSSARY OF TERMS

Accounts:

References to accounts mean a bank account and any other similar business relationship between a financial services business and a customer.

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:

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 owners:

The natural person(s) who ultimately own or control a relationship and/or the person on whose behalf the relationship is being conducted. Also those persons who exercise ultimate effective control over a legal person or arrangement.

Board:

References in the Handbook to the Board refer to the board of directors of the company and should be read as the senior management of the financial services business where the business is not a company, but is, for example, a branch or partnership.

Business relationship:

A continuing arrangement between the financial services business in question and another party, to facilitate the carrying out of transactions, in the course of such financial services business – (i) on a frequent, habitual, or regular basis; and (ii) where the monetary value of any transactions to be carried out in the course of the arrangement is not known on entering into the arrangement.

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 form, or has formed, a business relationship with a financial services business, or is seeking 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 enters into 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, any account files and business correspondence relating to a 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:

Includes not only individuals working under a contract of employment, but also includes temporary and contract staff.

Express trust:

A trust clearly created by the settlor, usually in the form of a document, e.g. a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangement (e.g. constructive trust).

FATF Recommendations:

The Forty Recommendations and the Nine Special Recommendations on Terrorist Financing 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 identification and verification 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) Bailiwick of Guernsey) Regulations, 2007.

Foreign counterparts:

Authorities in another country or territory that exercise similar responsibilities and functions to the domestic authority referenced.

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 on Countering Financial Crime and the Financing of Terrorism issued from time to time by the Guernsey Financial Services Commission.

Identification data:

Data, documents or information, in any form whatsoever, which is from a reliable and independent source.

Intermediary:

An introducer which meets the criteria for it to be treated as a customer set out in section 6.6 of the Handbook.

Introducer:

A financial services business which enters, on behalf of one or more third parties (underlying principals) who are also its customers, into a business relationship with another financial services business.

Legal arrangements:

Express trusts or other similar legal arrangements.

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.

Money laundering:

Covers all transactions and activities proposed or undertaken in order to conceal the origins

of criminal proceeds so that they appear to have originated from a legitimate source.

Occasional transactions:

These are transactions 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.

Recognised investment exchange:

An investment exchange which appears to the Commission to be situate in and recognised as an investment exchange within the meaning of the law relating to investment exchanges of:

(a) any member state of the European Economic Community; or

(b) any prescribed country or territory; or

(c) any country or territory specified in writing by the Commission in any particular case for any particular purpose.

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.

Relationship risk profile:

Contains the customer due diligence information on the customer/underlying principals, the purpose and intended nature of the relationship and the type, volume and value of activity that can be expected within the relationship.

Relevant employees:

Employees whose duties relate to the provision of financial services and anyone who is exposed to the risk of money laundering and terrorist financing including the Board and senior management.

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 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.

Terrorist financing:

The provision or receipt of money or property with the intention of it being used for the purposes of terrorism.

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:

Any document relating to a customer of a financial services business, which is a record of a financial, services business' dealings with a customer or person or entity acting on a customer's behalf.

Underlying principals:

Any person who is not a beneficial owner but who is a settlor, trustee, protector, beneficiary or any other persons who have control over the business relationship or occasional transaction, are collectively referred to as underlying principals.

Unique identifier:

Any unique combination of letters, numbers or symbols that refers to a specific originator.

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.