BERMUDA MONETARY AUTHORITY

BERMUDA

GUIDANCE NOTES FOR AML/ATF REGULATED FINANCIAL INSTITUTIONS ON ANTI-MONEY LAUNDERING AND ANTI-TERRORIST FINANCING 2016 (BERMUDA MONETARY AUTHORITY) NOTICE 2016

Take notice that pursuant to section 49M of the Proceeds of Crime Act 1997, the Minister of Legal Affairs has approved the Guidance Notes for AML/ATF Regulated Financial Institutions on Anti-Money Laundering and Anti-Terrorist Financing 2016. The Bermuda Monetary Authority has issued these Guidance Notes in accordance with its responsibilities under section 5(2) of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008. The full text of the Guidance Notes is available for download on the website of the Bermuda Monetary Authority at www.bma.bm

Made this 20th day of September 2016.

Jeremy Cox
Chief Executive Officer

BERMUDA MONETARY AUTHORITY

GUIDANCE NOTES

FOR ANTI-MONEY LAUNDERING & ANTI-TERRORIST FINANCING (AML/ATF) REGULATED FINANCIAL INSTITUTIONS ON AML/ATF

SEPTEMBER 2016

Pursuant to Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision & Enforcement) Act 2008 (Section 5(2))

CONTENTS

TABLE OF ABBREVIATIONS AND ACRONYMS 3
PREFACE 4
CHAPTER 1 - SENIOR MANAGEMENT RESPONSIBILITIES AND INTERNAL CONTROLS 11
CHAPTER 2 - RISK-BASED APPROACH 26
CHAPTER 3 - OVERVIEW OF CUSTOMER DUE DILIGENCE 41
CHAPTER 4 - STANDARD CUSTOMER DUE DILIGENCE MEASURES 48
CHAPTER 5 - NON-STANDARD CUSTOMER DUE DILIGENCE MEASURES 75
CHAPTER 6 - INTERNATIONAL SANCTIONS 127
CHAPTER 7 - ON-GOING MONITORING 143
CHAPTER 8 - WIRE TRANSFERS 148
CHAPTER 9 - SUSPICIOUS ACTIVITY REPORTING 162
CHAPTER 10 - EMPLOYEE TRAINING AND AWARENESS 178
CHAPTER 11 - RECORD-KEEPING 184
ANNEX I - SECTOR-SPECIFIC GUIDANCE NOTES FOR TRUST BUSINESS 190
ANNEX II - SECTOR-SPECIFIC GUIDANCE NOTES FOR INSURANCE BUSINESS 191
ANNEX III -SECTOR-SPECIFIC GUIDANCE NOTES FOR INVESTMENT BUSINESS 192
ANNEX IV - RISK FACTORS FOR POLITICALLY EXPOSED PERSONS 193
ANNEX V - REGULATORY AND SUPERVISORY RESPONSIBILITIES IN BERMUDA 198

TABLE OF ABBREVIATIONS AND ACRONYMS

AML/ATF	Anti-Money Laundering and Anti-Terrorism Financing
ATFA	Anti-Terrorism (Financial and Other Measures) Act 2004
ATM	Automated teller machine
BACS	Bankers Automated Clearing Services
BCBS	Basel Committee on Banking Supervision
BEI	Business entity identifier
BIC	Bank identifier code
BMA	Bermuda Monetary Authority
CDD	Customer due diligence
CHAPS	Clearing House Automated Payment System
FATF	Financial Action Task Force
FIA	Financial Intelligence Agency
IAIS	International Association of Insurance Supervisors
IBAN	International bank account number
IOSCO	International Organisation of Securities Commissions
IT	Information technology
LEI	Legal entity identifier
ML/TF	Money laundering and terrorist financing
MT	Message type
NAMLC	National Anti-Money Laundering Committee
NPM	New payment method
Orders	Overseas Territories Orders in Council
PEP	Politically exposed person
POCA	Proceeds of Crime Act 1997
PSP	Payment service provider
Regulations	Proceeds of Crime (Money Laundering) Regulations 1998
RFI	Regulated financial institution
SAR	Suspicious Activity Report
SEA Act	Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008
SWIFT	Society for Worldwide Interbank Financial Telecommunication
UN	United Nations

PREFACE

1. Bermuda has long-standing obligations for regulated financial institutions (RFIs) to maintain effective procedures to prevent and detect money laundering and terrorism financing (ML/TF). The offence of money laundering was first set out in the Proceeds of Crime Act 1997 (POCA 1997). Requirements to combat terrorism financing were first included in the Anti-Terrorism (Financial and Other Measures) Act 2004 (ATFA 2004). The original obligations for RFIs were established in the Proceeds of Crime (Money Laundering) Regulations 1998. Those regulations were repealed and replaced by the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 (the Regulations).

2. The Acts and Regulations described above established a new regulatory regime. The Financial Intelligence Agency Act 2007 created the Financial Intelligence Agency to receive and analyse suspicious activity reports. The Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 designated the Bermuda Monetary Authority (the BMA or Authority) as the supervisory body empowered to secure institutions' compliance with the Regulations, and obliges the Authority to publish the Guidance Notes. The National Anti-Money Laundering Committee (NAMLC), established under Section 49 of POCA 1997, plays an important role in developing Bermuda's national plan of action to combat money laundering and advises on the making of the anti-money laundering and anti-terrorist financing (AML/ATF) legislative framework. Additional information is available at www.namlc.bm.

3. Following an International Monetary Fund review of Bermuda in mid-2007 and a 2012 revision to the Financial Action Task Force (FATF) Recommendations, further amendments to the Regulations were adopted in 2015.

4. To assist RFIs in understanding and complying with Bermuda's AML/ATF Acts and Regulations, the Authority issued comprehensive guidance notes for AML/ATF-regulated financial institutions in January 1998 and October 2010. The Authority also issued AML/ATF Guidance Notes pertaining to wire transfers in October 2010 and trust business in February 2015. These Guidance Notes, issued in 2016, replace and supersede both sets of earlier Guidance Notes.

5. Bermuda recognises that its regulatory system is part of the global fight against ML/TF and other financial crime. Bermuda also acknowledges the need for all jurisdictions to operate their regulatory regimes cooperatively and compatibly with one another; doing so promotes an internationally level playing field for legitimate transactions while narrowing opportunities for ML/TF without detection.

Purpose and scope of these Guidance Notes

6. The purpose of these Guidance Notes is to assist AML/ATF regulated financial institutions to comply with Bermuda's AML/ATF legal and regulatory framework. The Guidance Notes:

- Outline the AML/ATF legal and regulatory framework for Bermuda institutions;
- Interpret the requirements of the relevant Acts and Regulations, including how implementation may be achieved in practice;
- Indicate good industry practice in the application of AML/ATF procedures using a proportionate, risk-based approach;
- Assist institutions in mitigating the risks of being used in connection with ML/TF; and
- Assist in detailing criteria to be followed by all Bermuda institutions where there is knowledge or suspicion to suspect ML/TF.

7. Against the backdrop of Bermuda's AML/ATF laws and regulations, these Guidance Notes set out guidelines for Bermuda institutions operating both in and outside Bermuda, and their directors, officers and employees.

8. This document provides guidance to institutions on:

- The responsibilities of senior management and internal controls (Chapter 1);
- The risk-based approach (Chapter 2);
- The application of standard and non-standard customer due diligence measures (Chapters 3, 4 and 5);
- Sanctions regimes (Chapter 6);
- On-going monitoring (Chapter 7);
- Wire transfers (Chapter 8);
- Suspicious activity reporting (Chapter 9);
- Employee training and awareness (Chapter 10); and
- Record-keeping (Chapter 11).

What is money laundering?

9. Money laundering is the process by which illegitimate or criminally derived money is made to appear legitimate. This result is achieved through a series of financial transactions designed to conceal the identity, source and/or destination of the criminally derived money. The process uses legal channels to conceal the criminal origins of illegal funds.

10. Money laundering generally involves three independent but sometimes simultaneous stages:

1. Placement: The physical placement or insertion of illegal money into the legitimate financial system. This stage deals primarily with cash proceeds of crime.
2. Layering: Separating the proceeds of criminal activity from their true origins by putting them through several layers of financial transactions.
3. Integration: This is the final stage of money laundering in which the criminal proceeds re-enter the legitimate economy, appearing to be derived from a legitimate source.

11. Under Bermuda law, money laundering involves the proceeds from any criminal conduct or any terrorist property. Criminal conduct includes all offences triable on indictment before the Supreme Court. Criminal conduct also includes all offences outside Bermuda that, had they occurred in Bermuda, would be triable on indictment before the Supreme Court. For more information, see Section 3 of the Proceeds of Crime Act 1997 and Section 8 of the Anti-Terrorism (Financial and Other Measures) Act 2004.

12. The activities carried out at all stages of the money laundering process are criminalised under Bermuda laws by virtue of Sections 43 through 45 of POCA 1997 and Section 8 of ATFA 2004. Sections 32, 33 and 230 of the Criminal Code also criminalise any attempt, conspiracy or incitement to commit any such offence.

13. Specific money laundering offences under Bermuda law include:

- Concealing or transferring proceeds of criminal conduct;
- Assisting another to retain proceeds of criminal conduct; and
- Acquisition, possession or use of proceeds of criminal conduct.

14. In addition, Sections 46–47 of POCA 1997 criminalise the following acts:

- Failure to disclose to the Financial Intelligence Agency (FIA) knowledge or suspicion of money laundering; and
- Tipping off a person other than the FIA by disclosing information likely to prejudice an investigation into money laundering.

15. Examples of money laundering include:

- Attempting to turn money raised through criminal activity into legitimate or clean money;
- Involvement with any criminal or terrorist property, or entering into arrangements to facilitate the retention or control of criminal or terrorist property; and
- The investment of proceeds of crime in further criminal activity or in financial products

and services.

16. Regardless of whether money laundering actually takes place, it is also a separate offence under the Regulations for institutions to fail to establish adequate and proportionate policies and procedures to prevent and detect money laundering.

17. The techniques used by money launderers constantly evolve, responding to the source, type and amount of funds to be laundered, and to the legislative, regulatory and law enforcement environment of the market in which the money launderer wishes to operate. Techniques employed may be local to a municipality, or they may be practiced commonly around the globe. One source of guidance on global money laundering methods is available at www.fatf-gafi.org.

What is terrorism financing?

18. Terrorism financing is the direct or indirect solicitation, collection or provision of financial or other material assistance for terrorism or for terrorist organisations or persons who encourage, plan or engage in terrorism.

19. Terrorism financing could involve funds raised from legitimate sources, such as personal or institutional donations and profits from businesses, or funds from criminal sources, such as the drug trade, arms smuggling, fraud, abduction and corruption. The primary objective of persons seeking to finance terrorism is not to conceal the source of funds, but to conceal the financing and the terrorist nature of the financed activity.

20. Terrorists and terrorist groups may have established links with organised crime groups and may use those links to move funds through the same channels as money launderers. Larger, property-owning terrorist groups may operate similarly to organised crime groups or governments, raising funds through various processes, including forms of 'taxation'. Other groups and individuals, however, may operate on a smaller scale, but nonetheless with devastating effect. Terrorism financing has two notable features:

- Terrorists are often funded from legitimately obtained income, including charitable donations and business profits; and
- Individual terrorist acts have been carried out using relatively small sums of money.

21. In seeking to evade detection by the authorities and to protect the identity of the ultimate beneficiaries, persons involved in terrorism financing use techniques similar to those employed by money launderers. Affected institutions have substantively the same duty to combat terrorism financing as they do to prevent money laundering.

22. The various activities involved in terrorism financing are criminalised by virtue of Sections 5 through 8 of ATFA 2004. Sections 32, 33 and 230 of the Criminal Code also criminalise any attempt, conspiracy or incitement to commit any such offence.

23. Specific terrorism financing offences under Bermuda law include:

- Fund raising for the purposes of terrorism;
- Soliciting, collecting or providing money or other property for the purposes of financing terrorist organisations or financing persons participating in terrorism;
- Using or possessing money or other property that is intended to be used for the purposes of terrorism; and
- Participating in arrangements to make money or property available for the purpose of terrorism.

24. In addition, ATFA 2004 criminalises the following acts:

- Failure to disclose to the FIA knowledge or suspicion of terrorist financing; and
- Tipping off a person other than the FIA by disclosing information likely to prejudice an investigation into terrorist financing.

25. Examples of terrorism financing include:

- Soliciting donations to a terrorist organisation;
- Purchasing antiquities or natural resources from a terrorist organisation; and
- Providing support to terrorist organisations.

26. Regardless of whether or not terrorist financing actually takes place, it is also a separate offence under the Regulations for institutions to fail to establish adequate and proportionate policies and procedures to prevent and detect terrorist financing.

27. Bermuda law criminalises the financing of terrorist actions that occur both in and outside Bermuda. Bermuda law also criminalises the financing of terrorist actions by both individuals and legal entities.

28. An important component of Bermuda's anti-terrorism financing system is the implementation of international sanctions against groups, entities and individuals designated as terrorists. For more information on international sanctions, see **Chapter 6: Sanctions Regimes**.

Who does the guidance address?

29. These Guidance Notes are addressed to AML/ATF-regulated financial institutions within the meaning of Section 2(1) of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 (SEA Act 2008). Approved by the Minister of Justice, these Guidance Notes are issued by the Authority under Section 5(2) of the SEA Act 2008.

30. These Guidance Notes are of direct relevance to all senior management, and compliance and reporting officers in institutions. The primary purpose of the notes is to provide guidance to those who set the institution's risk management policies and procedures for the prevention and detection of ML/TF.

31. Although the guidance will be relevant to operational areas, it is expected that these areas will be directed primarily by the institution's own detailed and specific internal arrangements, tailored by senior management to mitigate the risks identified by the institution's own risk assessment processes.

Status of the guidance

32. The Court, or the Authority, as the case may be, in determining whether a person is in breach of a relevant provision of the Acts or Regulations, is required to consider whether a person has followed any relevant guidance approved by the Minister of Justice and issued by the Authority. Requirements of the Court and the Authority are detailed in the provisions of Section 49A of POCA 1997, regulation 19(2) of the Regulations, Section 12(B) of, and paragraph 1(6) of Part I of Schedule I to ATFA 2004 and Section 20(6) of the SEA Act 2008.

33. Departures from this guidance, and the rationale for so doing, should be documented, and institutions should stand prepared to justify departures to authorities such as the BMA.

How should the guidance be used?

34. This guidance interprets the laws and regulations of Bermuda to assist institutions in meeting their AML/ATF obligations. The Guidance Notes do not address every requirement. Institutions must therefore rely first and foremost on the laws and regulations themselves.

35. These Guidance Notes are not intended to provide an exhaustive account of appropriate and effective policies, procedures and controls to prevent and detect ML/TF.

36. Each institution must assess the ML/TF risks to which it is exposed, and tailor its AML/ATF policies, procedures and controls to ensure adequate and proportionate mitigation of all risks.

37. The Authority expects institutions that it supervises to address their risk management in a thoughtful and considered way, and to establish and maintain policies, procedures and controls that are appropriate and proportionate to the risks identified.

38. Although these Guidance Notes generally provide a sound basis for institutions to meet their legal and regulatory obligations, effective risk mitigation may require additional measures beyond those set forth herein.

39. When a provision of the Acts or Regulations is directly described in the text of the guidance, the Guidance Notes use the term **"must"** to indicate that the provision is mandatory.

40. In other cases, the guidance uses the term **"should"** to indicate ways in which the requirements of the Acts or Regulations may be satisfied, while allowing for alternative means, provided that those alternatives effectively accomplish the same objectives.

CHAPTER 1 - SENIOR MANAGEMENT RESPONSIBILITIES AND INTERNAL CONTROLS

Introduction

1.1 This chapter provides guidance for senior management to establish AML/ATF policies and procedures in line with the Acts and Regulations of Bermuda.

1.2 The responsibilities for senior management of a Regulated Financial Institution (RFI) are governed primarily by the Proceeds of Crime Act 1997, Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008, Anti-Terrorism (Financial and Other Measures) Act 2004, and Regulations 16, 17 and 19.

1.3 This chapter also provides guidance on internal controls relating to financial sector group policies, employee screening and independent auditing that are appropriate for an RFI to meet its obligations under the AML/ATF Acts and Regulations.

1.4 The internal control requirements for RFIs are governed primarily by Regulations 12, 16 and 18.

1.5 An RFI's involvement in money laundering or terrorism financing (ML/TF), whether intentional, knowing, inadvertent or negligent, creates legal, regulatory and reputational risks.

1.6 Under the Acts and Regulations of Bermuda, senior management must ensure that the RFI's policies, procedures and controls for preventing and detecting ML/TF are appropriately designed and implemented. The RFI's policies, procedures and controls must:

- Assess the ML/TF risks the RFI faces;
- Consider how those risks best can be addressed; and
- Effectively mitigate the risk of the RFI being used in connection with ML/TF.

1.7 Senior management must apply a risk-based approach for the purposes of preventing and detecting ML/TF. In doing so, RFIs may draw upon experience applying proportionate, risk-based policies across different aspects of its business.

1.8 Under a risk-based approach, RFIs should identify and assign risk ratings to their customers, products, services, transactions, delivery channels, outsourcing arrangements and geographic connections. AML/ATF policies, procedures and controls should be applied in a manner that

allocates compliance resources in proportion to the risks identified; this approach is intended to increase effectiveness in a cost-effective manner. See **Chapter 2: Risk-Based Approach**.

1.9 Senior management should ensure that the RFI's risk ratings and risk management policies, procedures and controls are responsive to any information the Authority or other competent authority provides to the RFI with regard to Bermuda's ML/TF national risk assessment.

1.10 Senior management must be fully engaged in decision-making processes, and must take ownership of the risk-based approach. Senior management is accountable where the approach is determined to be inadequate.

The AML/ATF framework in Bermuda

1.11 A full, up-to-date listing of Bermuda legislation is available at www.bermudalaws.bm. Key elements of the AML/ATF framework in Bermuda include:

- Revenue Act 1898
- Criminal Code Act 1907
- Criminal Justice (International Cooperation) (Bermuda) Act 1994
- Proceeds of Crime Act 1997
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008
- Anti-Terrorism (Financial and Other Measures) Act 2004
- Financial Intelligence Agency Act 2007
- Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008
- Proceeds of Crime Appeal Tribunal Regulations 2009
- Proceeds of Crime (Designated Countries and Territories) Order 1998
- The Extradition (Overseas Territories) Order 2002
- Anti-Terrorism (Financial and Other Measures) (Business in Regulated Sector) Order 2008
- The Terrorist Asset-Freezing etc. Act 2010 (Overseas Territories) Order 2011 (An unofficial Consolidation of the Terrorist Asset-Freezing etc. Act 2010 and the above Order is provided on the website for ease of reference)
- Guidance Notes for AML/ATF Regulated Financial Institutions on Anti-Money Laundering & Anti-Terrorist Financing
- International Sanctions Act 2003 and International Sanctions Regulations 2013

1.12 The AML/ATF framework in Bermuda has been revised pursuant to the following international standards and requirements:

- The FATF Recommendations (as amended February 2012).
- UN Security Council Resolutions 1267 (1999), 1373 (2001), and subsequent resolutions 1333 (2000), 1390 (2002), 1455 (2003), 1526 (2004), 1617 (2005), 1735 (2006), 1822 (2008), 1904 (2009), 1989 (2011), 2083 (2012), and 2161 (2014).

1.13 Bermuda RFIs may also find the following international regulatory pronouncements useful:

Basel Committee on Banking Supervision (BCBS)

- Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-Border Wire Transfers (May 2009)
- Sound Management of Risks Related to Money Laundering and Financing of Terrorism (January 2014)

International Association of Insurance Supervisors (IAIS)

- Guidance Paper 5 on Anti-Money Laundering and Combating the Financing of Terrorism (October 2004)
- Issues Paper on Combating Bribery and Corruption (October 2004)
- Examples of Money Laundering and Suspicious Transactions Involving Insurance (October 2014)

International Organisation of Securities Commissions (IOSCO)

- Anti-Money Laundering Guidance for Collective Investment Schemes (October 2005)

Wolfsberg AML Principles

- Available at www.wolfsberg-principles.com

FATF Guidance

- Available at www.fatf-gafi.org

Extra-territorial matters

1.14 Where an RFI has a listing, or has activities in, or is linked to a country or territory other than Bermuda, whether through a branch, subsidiary, associated company or provision of correspondent banking services, it is possible that, in addition to the Acts and Regulations of Bermuda, sanctions and AML/ATF measures of the other country or territory also apply to activities of the RFI. RFIs with overseas correspondent banking relationships need to be aware of the jurisdictional requirements applicable to those clearing institutions and monitor

whether they stay abreast of the full range of AML/ATF requirements in place and the potential for modifications and enhancements in those requirements. Senior management should obtain advice on the extent to which the RFI's activities may be affected in this manner.

Regulatory priorities

1.15 No single Bermuda body has overall responsibility for combating money laundering or terrorist financing. The division of responsibilities is described in Appendix II.

1.16 Regulation of and guidance to RFIs is provided by the BMA.

1.17 The Regulations apply to a range of specified RFIs carrying on business in Bermuda. POCA 1997 and ATFA 2004 criminalise ML/TF, respectively. RFIs are now legally obliged to put in place effective measures to minimise the chance of involvement with the proceeds of any crime or any terrorist property.

1.18 The BMA's objectives are to use regulatory measures to:

- Monitor AML/ATF regulated financial institutions to ensure full compliance with Bermuda's legal and regulatory framework;
- Assist with the prevention and detection of financial crime; and
- Deter and disrupt criminal and terrorist activity by increasing the risk that perpetrators are apprehended, and by reducing the benefit perpetrators receive from their crimes.

1.19 In order to deliver these objectives successfully, the BMA's actions in this area are underpinned by three key organising principles:

Effectiveness – Maximise the impact of AML/ATF measures on criminality and terrorism by:

- Building knowledge of commercially effective compliance strategies that drive continuous improvement; and
- Ensuring that all RFIs make full use of the opportunities provided by the Acts and Regulations to prevent and detect ML/TF.

Proportionality – Ensure that the benefits of intervention are justified and that they outweigh the costs by:

- Entrenching the risk-based approach.

Engagement – Work collaboratively in partnership with all stakeholders in Government and the private sector, both at home and abroad, in order to:

- Share data across the AML/ATF community to reduce harm; and
- Engage internationally to assist in delivery of a global solution to this global problem.

General legal and regulatory obligations

1.20 For the purposes of these Guidance Notes, senior management refers to one or more of the following:

- The board of directors as a single decision-making body;
- One or more appropriate directors;
- A "chief executive" who, either alone or jointly with one or more persons, is responsible under the immediate authority of the directors for the conduct of the business of the RFI;
- A "senior executive" other than a chief executive who, under the immediate authority of a director or chief executive of the RFI, exercises managerial functions or is responsible for maintaining accounts or other records of the RFI.

1.21 Senior management in all RFIs must:

- Ensure compliance with the Acts and Regulations;
- Identify, assess and effectively mitigate the ML/TF risks to its customers, products, services, transactions, delivery channels, outsourcing arrangements and geographic connections;
- Ensure that AML/ATF risk assessment framework remains relevant and appropriate given the RFI's risk profile;
- Appoint a Compliance Officer at the managerial level to oversee the establishment, maintenance and effectiveness of the RFI's AML/ATF policies, procedures and controls;
- Appoint a Reporting Officer to process disclosures;
- Screen employees against high standards;
- Ensure that adequate resources are devoted to the RFI's AML/ATF policies, procedures and controls;
- Audit and periodically test the RFI's AML/ATF policies, procedures and controls for effectiveness; and
- Recognise potential personal liability if legal obligations not met.

1.22 Senior management of any RFI is responsible for managing its business effectively. Certain obligations are placed on all RFIs subject to the Regulations; fulfilling these responsibilities falls to senior management as a whole. See Regulation 16.

1.23 The Regulations place a general obligation on RFIs to establish appropriate and risk-sensitive policies and procedures to prevent and detect ML/TF. An RFI that fails to comply with this obligation is subject to regulatory enforcement action. See Regulations 16 and 19(1).

1.24 The offences of money laundering under POCA 1997 and the obligation to report knowledge or suspicion of possible money laundering affect all persons, not only RFIs. Similar offences and obligations under ATFA 2004 also affect all persons, not only RFIs. In addition, the Regulations require RFIs to take appropriate measures so that all relevant employees are made aware of the Acts and Regulations relating to ML/TF, and to regularly train them how to recognise and deal with transactions that may be related to money laundering or terrorism financing. See Regulations 17 and 18, Section 46 of POCA 1997, and Schedule 1 Part 1 of ATFA 2004.

1.25 Where a corporate, partnership or unincorporated association is guilty of an offence under POCA 1997 and/or ATFA 2004 and that offence is proved to have been committed with the consent or connivance of, or due to negligence by, any director, manager, secretary or similar officer of the entity or any person who was purporting to act in any such capacity, he, as well as the legal entity, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly. See Regulation 19(1), Section 56 of POCA 1997 and Section 5B of ATFA 2004.

Criminal and civil penalties

1.26 RFIs should be aware that Regulation 19 provides that failure to comply with the requirements of specified Regulations is a criminal offence and carries with it significant penalties. On summary conviction, the penalty is a fine of up to $50,000. Where conviction occurs on indictment, penalties include a fine of up to $750,000, imprisonment for a term of two years, or both.

1.27 Section 20 of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 empowers the BMA to impose a penalty on an AML/ATF-RFI of up to $500,000 for each failure to comply with specified Regulations. Total penalties therefore may be well above $500,000. For full details concerning the civil penalties process, see Chapter 4 of the Act. The Act also provides for criminal offences. For example, Section 33 creates offences, which carry significant penalties if convicted, whether summarily or on indictment. The offences include carrying on business without being registered pursuant to Section 9 of the Act. The BMA has published a Statement of Principles, which states its approach in exercising its powers.

1.28 Regulation 19(4) states that anyone convicted of an offence under Regulation 19 shall not also be liable to a civil fine imposed by or under any other statutory provision in relation to the same matter.

Formal AML/ATF policy statement

1.29 Senior management should adopt and document a formal AML/ATF policy statement in relation to the prevention and detection of ML/TF.

1.30 The policy statement should state how senior management carries out its responsibility to ensure that the RFI's policies, procedures and controls are appropriately designed and implemented.

1.31 The policy statement should also set out how senior management undertakes its assessment of the ML/TF risks the RFI faces, and how these risks are to be managed.

1.32 A high level AML/ATF policy statement should focus employees on the need to be constantly aware of ML/TF risks, and how they are to be managed.

1.33 An effective AML/ATF policy will provide a framework of direction to the RFI and its employees, and will identify specific individuals and functions responsible for implementing particular aspects of the RFI's detailed policies, procedures and controls.

1.34 The policy statement might include, but not be limited to, such matters as:

<u>Guiding principles:</u>

- An unequivocal statement of the culture and values that have been adopted by the RFI to prevent and detect financial crime;
- A commitment to hiring and retaining only those employees who follow the principles;
- A commitment to ensuring that employees are trained in an on-going and risk-sensitive manner and are knowledgeable about the Acts and Regulations and their obligations thereunder;
- A commitment to ensuring that the RFI accepts only those customers whose identity has been verified;
- A commitment to the RFI 'knowing its customers' appropriately, both at the time of acceptance and throughout the business relationship, by taking appropriate steps to verify the customer's identity, verify beneficial ownership and understand the purpose and intended nature of the business relationship with the RFI;

- A commitment to periodic independent auditing to test the RFI's AML/ATF policies, procedures and controls;
- A commitment to address shortcomings in a timely manner; and
- A commitment that employees promptly report their suspicions internally.

Risk mitigation procedures:

- A summary of the RFI's approach to assessing and managing its ML/TF risks, including a statement of the RFI's risk tolerance;
- Identification of specific individuals and functions responsible for implementing particular aspects of the RFI's detailed policies, procedures and controls;
- A summary of the RFI's procedures for carrying out appropriate identification, verification and monitoring checks on the basis of its risk methodologies; and
- A summary of the appropriate monitoring arrangements in place to ensure that the RFI's policies, procedures and controls are being carried out effectively and remain proportional to evolving risk factors.

1.35 The policy statement should be tailored to the circumstances of the RFI. The use of a generic document is likely to reflect adversely on the level of consideration that senior management has given to the RFI's AML/ATF obligations and the ML/TF risks it faces.

Compliance Officer and Reporting Officer

1.36 RFIs must appoint a Compliance Officer, who must be at the managerial level, and who must have the authority to:

- Oversee the establishment, maintenance and effectiveness of the RFI's AML/ATF policies, procedures and controls;
- Monitor compliance with the relevant Acts, Regulations and guidance; and
- Access all necessary records in a timely manner.

1.37 RFIs must also appoint a Reporting Officer with the authority to carry out the following duties:

- Receive suspicious activity disclosures from the RFI's employees;
- Access all necessary records in a timely manner;
- Make final determinations on whether disclosures should be reported to the FIA; and
- Where appropriate, make external reports to the FIA.

1.38 The Reporting Officer may be, but is not required to be a member of senior management. At a minimum, however, the Reporting Officer should be a qualified member of the RFI's staff.

1.39 Senior management of the RFI should ensure that the Reporting Officer has the autonomy to make a final decision as to whether to file a suspicious activity report.

1.40 The Reporting Officer should have direct access to the BMA and, where appropriate, law enforcement agencies, to ensure that any suspicious activity is properly reported as soon as is practicable. The Reporting Officer must be free to liaise with the Financial Intelligence Agency on any question of whether to proceed with a transaction.

1.41 Senior management of the RFI should ensure that the Reporting Officer has sufficient resources, including time, employees and technology and direct access to and support from senior management. In the case of the Reporting Officer's absence, arrangements should be made to ensure proper coverage of duties, and awareness among employees of any changes to the procedures to follow when suspicion arises.

1.42 Senior management of the RFI should ensure that the Reporting Officer has timely access to the RFI's relevant business information, including, but not limited to:

- Customer due diligence and on-going monitoring records; and
- Transaction details.

1.43 The Compliance Officer and Reporting Officer may be the same individual.

1.44 Where they are not the same person, the Compliance Officer and the Reporting Officer should maintain open lines of communication and understand each other's role and responsibilities. The relationship should be clearly defined and documented.

1.45 Depending on the size of the RFI, or by the structure of a financial sector group, the duties of the Compliance Officer and/or Reporting Officer may be delegated to additional senior, appropriately qualified individuals within the RFI or group. The appointment of one or more permanent deputy Reporting Officers may also be necessary. In these cases, the principal or group Reporting Officer should ensure that roles and responsibilities are clearly defined, and that employees know where to direct reports of suspicions.

1.46 Senior management should ensure that all relevant employees of the RFI are aware of the identity of the Reporting Officer and any deputies, and that all relevant employees are aware of the procedures to follow when suspicion arises.

1.47 The role, standing and competence of the Compliance Officer and the Reporting Officer, and the manner in which the RFI's policies, procedures and controls are designed and implemented, impact directly on the effectiveness of an RFI's AML/ATF arrangements, and the degree to which the RFI is in compliance with the Acts and Regulations of Bermuda.

1.48 RFIs should notify the BMA of the name and contact information of the Compliance Officer, Reporting Officer and any deputies, and of any subsequent changes. Receipt of such information enhances the BMA's ability to communicate effectively with RFIs. Information should be sent via e-mail to: **aml@bma.bm**

1.49 For additional information regarding the duties of the Reporting Officer, see **Chapter 9: Suspicious Activity Reporting**.

Periodic report

1.50 At least once a year, the Compliance Officer should report on the operation and effectiveness of the RFI's AML/ATF policies, procedures and controls. Senior management should determine the scope and frequency of information it feels is necessary to discharge its responsibilities; an RFI may determine that the Compliance Officer needs to report to senior management frequently.

1.51 The periodic report may include:

- The means by which the effectiveness of the RFI's policies, procedures and controls has been managed and tested;
- Identification of compliance deficiencies and details of action taken or proposed to address any such deficiencies;
- Failure to apply Bermuda requirements in branches and subsidiaries, any advice received from the BMA and details of action taken;
- The number of internal disclosures to the Reporting Officer and the number of subsequent external reports submitted to the FIA, any perceived deficiencies in internal or external reporting procedures, and the nature of action taken or proposed to address such deficiencies, such as customer due diligence reviews, on-going monitoring reviews/projects, AML/ATF training taken by the Compliance Officer and/or Reporting Officer;
- Information concerning the training programme for the preceding year, which employees have received training, the methods of training and the nature of the training;
- Changes made or proposed in respect of new or revised Acts, Regulations or guidance;

- A summary of risk assessments conducted or updated with regard to customers, products, services, transactions, delivery channels, outsourcing arrangements and geographic connections.
- The nature of actions taken with regards to jurisdictions that do not sufficiently apply the FATF Recommendations, or which are the subject of international countermeasures, and the measures taken to manage and monitor business relationships connected with such jurisdictions; and
- Any recommendations concerning additional resource requirements to ensure effective compliance with the RFI's statutory and regulatory obligations.

1.52 Where an RFI is part of a group or involved in multiple jurisdictions, a consolidated report may be appropriate.

1.53 At the time senior management receives a report on the operation and effectiveness of the RFI's AML/ATF policies, procedures and controls, it should consider the report and take any and all necessary actions in a timely manner to remedy any deficiencies identified.

Internal controls

1.54 In addition to a formal AML/ATF policy statement, RFIs must establish and maintain detailed policies, procedures and controls that are adequate and appropriate to forestall and prevent operations related to ML/TF.

1.55 All such policies, procedures and controls must be risk sensitive, based on a variety of factors, including:

- The nature, scale and complexity of the RFI's business;
- The diversity of its operations, including the RFI's geographical connections;
- Its customers;
- Its products, services, and delivery channels;
- Its transactions, including their volume and size; and
- The degree of risk assessed in each area of its operation.

1.56 More specific requirements for an RFI's detailed policies, procedures and controls are set forth in **Chapters 2 through 11** of these guidance notes.

Application of group policies

1.57 Where a Bermuda RFI has branches, subsidiaries or representative offices located in a country or territory other than Bermuda, it must communicate its AML/ATF policies and procedures to all such entities.

1.58 Bermuda RFIs must also ensure that all branches, subsidiaries and representative offices located outside Bermuda apply AML/ATF measures at least equivalent to those set out in the Acts and Regulations.

1.59 To accomplish paragraphs 1.57 and 1.58 above, RFIs should consider adopting group-wide AML/ATF policies and procedures.

1.60 A financial sector group's policies and procedures must provide for the group-wide sharing of information required for the purposes of Customer Due Diligence (CDD), ongoing monitoring, record-keeping and other ML/TF risk management policies, procedures and controls.

1.61 Group-level AML/ATF functions should be provided with customer, account and transaction information from branches and subsidiaries where required for AML/ATF purposes.

1.62 RFIs should establish and maintain adequate safeguards on the confidentiality and use of the information exchanged.

1.63 Individual RFIs and financial sector groups should have access to customer, account and transaction information from branches and subsidiaries where necessary for the purposes of on-going monitoring.

1.64 Where operational activities of a Bermuda RFI are undertaken by employees in other jurisdictions, those employees should be subject to the same AML/ATF policies and procedures applied to Bermuda employees. Senior management should ensure that all suspicious transactions or activities linked with a Bermuda RFI or Bermuda person are reported to the Reporting Officer in Bermuda.

1.65 Where the AML/ATF standards in the country or territory hosting a branch or subsidiary are more rigorous than those required by the Acts and Regulations, RFIs should ensure that those higher standards are implemented.

1.66 Where the law of a country or territory other than Bermuda does not permit the application of AML/ATF measures at least equivalent to those in Bermuda, the RFI must inform the BMA accordingly, and must take additional measures to effectively manage the risks of ML/TF. See Regulation 12(2).

1.67 RFIs that have informed the BMA that the law of a country or territory other than Bermuda does not permit the application of AML/ATF measures at least equivalent to those in Bermuda should follow any advice, recommendations or directions from the BMA as to the action to take.

1.68 Where an RFI finds that additional measures are insufficient for the purposes of effectively mitigating the risks of ML/TF, and particularly where effective AML/ATF policies, procedures or controls are likely to be impeded by confidentiality, secrecy, privacy or data protection restrictions, RFIs must inform the BMA, which may require that the relationship be terminated. The RFI should follow any advice, recommendations or directions the BMA or other competent authority provides as to the action to take.

1.69 Additional guidance regarding reliance on third parties and outsourcing arrangements is contained in **Chapter 5: Non-Standard Customer Due Diligence Measures**.

Employee screening

1.70 An RFI's AML/ATF policies and procedures must require relevant employees to be screened against high standards as noted below.

1.71 For the purposes of these guidance notes, the term 'employee' includes any person working for an RFI, including persons working under a contract of employment and persons working under a contract for services. A relevant employee is one who:

- At any time in the course of his duties has or may have access to any information which may be relevant in determining whether funds or assets are the proceeds of crime, or that a person is involved in money laundering or terrorist financing; or
- At any time plays a role in implementing and monitoring compliance with AML/ATF requirements.

1.72 Where employees of any third parties carry out work in relation to an RFI under an outsourcing agreement, the RFI should have procedures to satisfy itself as to the effectiveness of the screening procedures of the third party in ensuring employee competence and probity.

1.73 To ensure that employees are of the standard of competence and probity proper for their role, RFIs should:

- Request and verify appropriate references for the employee at the time of recruitment;

- Verify the employee's employment history, qualifications and professional memberships;
- Request and verify the details of any regulatory action taken against the employee, or any action taken by a professional body;
- Request and verify the details of any criminal convictions, or the absence of any such convictions by, e.g. requesting a police report from the appropriate jurisdiction(s);
- Consult the most up-to-date lists of specified countries and persons against whom sanctions have been imposed by the United Nations, the European Union or other relevant body or jurisdiction on the grounds of suspected or known involvement in terrorist or other illegal activity.

1.74 RFIs should document, or record electronically, the steps taken to satisfy these requirements, including the information and verifications obtained. RFIs should also document, or record electronically, any situation where an employee has been hired despite the RFI's inability to obtain all relevant information. In such cases, RFIs should include the reasons why all relevant information was not obtained, an appropriate risk-based rationale for the exception, and details regarding alternative screening methods undertaken. All related records should be retained in accordance with the guidance provided in **Chapter 11: Record Keeping**.

Independent audit

1.75 The independent audit function should provide for an internal audit of the RFI's AML/ATF policies, procedures and controls. RFIs should conduct an audit to monitor and sample test the implementation, integrity and effectiveness of their AML/ATF policies, procedures and controls on a regular basis. This means at least once a year and more frequently when senior management becomes aware of any gap or weakness in the AML/ATF policies, procedures or controls, or when senior management deems it necessary due to the RFI's assessment of the risks it faces.

1.76 Where appropriate, having regard to the risk of ML/TF and the size of the business, the audit may be undertaken by the compliance and/or internal auditing departments. The audit should be adequately resourced to help ensure AML/ATF compliance and it should be carried out independently of any general audit. The independent audit does not require the establishment of a separate dedicated department or section, only that the audit itself is sufficiently separate and distinct, focused solely on AML/ATF matters and not found within the general audit.

1.77 The audit function should:

- Evaluate the risk ratings the RFI has assigned with respect to its size, customers, products, services, transactions, delivery channels, outsourcing arrangements and geographic connections;
- Assess the adequacy of the RFI's AML/ATF policies, procedures and controls including:
  - Risk assessment;
  - Customer due diligence;
  - Risk mitigation and other measures to manage higher risks;
  - On-going monitoring;
  - Detecting and reporting suspicious activity;
  - Record-keeping and retention; and
  - Reliance and outsourcing relationships;
- Test compliance with the relevant laws and regulations;
- Test the AML/ATF controls for the RFI's transactions and activities, with an emphasis on higher-risk areas;
- Assess employees' knowledge of the relevant Bermuda Acts, Regulations and guidance, the RFI's policies and procedures and the role of each employee within the RFI; and
- Assess the adequacy, accuracy and completeness of employee training and awareness programmes.

1.78 The audit should be documented, or recorded electronically, and retained in accordance with the guidance provided in **Chapter 11**.

1.79 The results of the audit should be included in reports to senior management and the Board for timely action.

CHAPTER 2 - RISK-BASED APPROACH

Introduction

2.1 This chapter provides guidance on using a risk-based approach to mitigate the risks of an RFI being used in connection with ML/TF.

2.2 The responsibilities of RFIs to utilise the risk-based approach in meeting their AML/ATF obligations are governed primarily by Regulation 16.

2.3 RFIs must employ a risk-based approach in determining:

- Appropriate levels of CDD measures;
- Proportionate measures to prevent the abuse of the RFI's products, services and delivery channels for ML/TF purposes;
- The scope and frequency of on-going monitoring; and
- Measures for detecting and reporting suspicious activity.

2.4 This chapter is not intended to be used as a checklist. An RFI may find that portions of this chapter are not relevant to its business, or that this chapter does not address specific risks associated with its business.

2.5 Each RFI should manage its ML/TF risks in an analytical and considered way, and establish and maintain policies, procedures and controls that are specific, appropriate and proportionate to the risks its senior management identifies.

2.6 Policies, procedures and controls may not always prevent and detect all ML/TF. However, a risk-based approach allows RFIs to balance the cost of AML/ATF compliance resources with a realistic assessment of the risk of the RFI being used in connection with ML/TF. A risk-based approach focuses resources and efforts where they are needed and where they have the greatest impact.

The concept of risk

2.7 Risk can be defined as a combination of the following:

- The **threat** of an event;
- **Vulnerability** to such a threat; and
- The **consequence** of the threatened event actually taking place.

2.8 In simple terms, risk is a combination of the likelihood that something might occur and the consequence of such an occurrence.

Risk management

2.9 Risk management is the process of measuring risks and applying appropriate mitigation measures to minimise risks. Senior management of most RFIs have experience managing the RFI's affairs with regard to the risks inherent in the business and the effectiveness of controls to manage those risks. In the context of AML/ATF compliance, risk management is a tool to assist senior management in making decisions about the need for and allocation of AML/ATF compliance resources.

Inherent and residual risks

2.10 It is important to distinguish between inherent risk and residual risk. Inherent risk is the intrinsic risk of an event or circumstance that exists before the application of mitigation measures. Residual risk, by contrast, is the level of risk that remains after the application of mitigation measures.

National risk assessment

2.11 Bermudian authorities periodically conduct a national risk assessment to identify, measure and plan responses to the ML/TF risks that Bermuda faces. The national risk assessment benefits from inputs from industry, and results in outputs useful to industry.

2.12 Senior management should ensure that the RFI's risk ratings and risk management policies, procedures and controls are responsive to any information the Authority or other competent authority provides to the RFI with regard to Bermuda's ML/TF national risk assessment.

Business risk assessment

2.13 Under the risk-based approach, an RFI should be able to demonstrate that it follows appropriate and documented procedures for assigning risk ratings to each business relationship it accepts or maintains and each occasional transaction it conducts.

2.14 The purpose of an RFI applying a risk-based approach is to ensure that its compliance resources are allocated to the risk areas where they are needed and where they have the greatest impact in preventing and suppressing ML/TF.

2.15 The risk assessments that each RFI conducts should be appropriate to the nature, size, turnover and complexity of the RFI.

2.16 Some smaller RFIs with a limited range of customers and minimal products or services may be able to be satisfied, on reasonable grounds, that standardised profiles for particular combinations of customers and services are appropriate. A focus of such RFIs' efforts should be on those combinations of customers and services that fall outside of any standardised profile.

2.17 RFIs with a diverse customer base, or with a variety of products, services and delivery channels, should develop a more structured and rigorous risk-based approach. Such RFIs likely require dedicated compliance employees and more detailed policies, procedures and controls to demonstrate that judgment has been exercised on more granular or individual basis, rather than on a generic or standardized basis.

2.18 Assessing groups of clients or business relationships that share similar characteristics is acceptable provided that the RFI can demonstrate that the groupings are sufficiently logical and specific to reflect the reality of the RFI's business.

2.19 Regardless of its nature, size, turnover and complexity, each RFI should begin assessing the risks it faces either before commencing business, or as soon as is reasonably practicable afterward.

2.20 Each RFI should document its risk-related policies, procedures and controls and should ensure that the methodology and results of its risk assessments are regularly reviewed and amended to keep them up to date. All related records should be documented, or recorded electronically, and retained in accordance with the guidance provided in **Chapter 11**.

2.21 Each RFI should ensure that it has sufficient capacity and expertise to manage the risks it faces. As risks and understandings of risk evolve, a RFI's capacity and expertise should also evolve proportionally.

2.22 Each RFI should ensure that its risk assessment methodology and the results of its risk assessments are readily available to be shared with competent authorities.

2.23 The appropriate approach in any given case is ultimately a question of judgment by senior management. At all times, an RFI's risk assessments should be objectively justifiable and sufficiently robust so as to demonstrate that the business acted reasonably.

2.24 One way for an RFI to meet its obligations to apply AML/ATF compliance resources, using a risk-based approach, is to regularly engage in a six-step business risk assessment cycle:

I. **Identify and assess inherent risks**: Consider all relevant risk factors with regard to the RFI's customers, products, services, transactions, delivery channels, third party service providers and geographic connections in order to assign inherent risk ratings;

II. **Establish risk tolerance**: Determine the level of risk the business is willing to accept;

III. **Establish risk mitigation measures**: Develop and document proportionate and effective policies, procedures and controls in order to minimise and manage the risks that have been assessed;

IV. **Evaluate residual risks**: Determine the level of risk remaining after taking mitigation measures into consideration;

V. **Implement risk mitigation measures**: Apply the risk mitigation policies, procedures and controls that have been developed and documented;

VI. **Monitor and review risks**: Maintain risk assessment information and risk ratings up to date, and regularly review, test and improve the policies, procedures and controls put in place.

I. Identify and assess inherent risks

2.25 RFIs should identify and assess the inherent risks they face with regard to customers, products, services, transactions, delivery channels, third party service providers and geographic connections.

2.26 Inherent risks are the intrinsic risks of an event or circumstance that exist before the application of mitigation measures.

2.27 RFIs should consider all relevant information when identifying and assessing inherent risks. Such information includes, but is not limited to:

- Business information held by the RFI, including customer information and transaction information;
- Publically available information, such as that in court records or reliable media;
- Commercially available information, such as electronic databases;

- Local, domestic and international reports and guidance regarding ML/TF threats, vulnerabilities, trends and typologies.

2.28 These guidance notes do not prescribe a particular methodology for the assessment of risks. The following is one example of a risk assessment methodology. Each RFI must ensure that the methodology it uses is appropriately adapted to its particular needs.

2.29 As a general matter, RFIs should consider the three factors that comprise risk:

- Threat (t)
- Vulnerability (v)
- Consequence (c)

2.30 As a mathematical function, risk (r) is calculated as follows: $r = (t*v) * c$.

2.31 When combined, threat and vulnerability (t*v) form likelihood (l).

2.32 Paragraphs 2.33 through 2.46 address threats, inherent vulnerabilities and likelihood. Paragraphs 2.67 through 2.74 address residual vulnerabilities and their impact on likelihood. Consequences are addressed in paragraphs 2.50 through 2.59.

Threat

2.33 A threat is a person, object or activity with the potential to cause harm. In the AML/ATF context, a threat is the demand for ML/TF services by criminals, terrorists and their facilitators. Such demand is influenced by the types and scale of crimes that produce proceeds in a jurisdiction and the volume of proceeds of foreign crimes that enter the jurisdiction. Although the Bermudian authorities use the national risk assessment process to identify threats at the national level, RFIs should independently assess the threat of customers seeking to attempt ML/TF at the business or transactional level. Customers who pose a greater threat of ML/TF are higher-risk customers.

2.34 An RFI should assign risk ratings to each customer, based upon all information available.

2.35 The following is a non-exhaustive list of factors that may increase the risk rating assigned to a customer:

- A customer whose identification is difficult to obtain or verify;
- A customer who has been accepted with no face-to-face interaction;
- A customer seeking to deposit significant amounts of cash;

- A customer seeking a product or service that is unusual for such a customer;
- A customer with an unusually or unnecessarily complex or non-transparent ownership structure;
- A customer who requests undue levels of secrecy, speed, volume or frequency when transacting;
- A customer whose origin of wealth or source of funds cannot be easily verified or with regard to whom the audit trail has been deliberately broken or unnecessarily layered;
- A customer who is a politically exposed person;
- A customer who is from, in, or seeking to conduct business in or through, a high-risk jurisdiction;
- A customer with regard to whom a suspicious activity report was considered or filed;
- A customer who appears in reliable media, court records, or electronic databases due to alleged or proven links with criminal activity.

2.36 An RFI's risk ratings should differentiate those customers who pose a greater threat from those who pose a lower threat. This may be accomplished in a number of ways. One approach is to assign a customer risk rating of high, medium or low.

Vulnerability

2.37 A vulnerability is a thing that may be exploited by a threat or that may support or facilitate a threat's activities. In the AML/ATF context, vulnerabilities are an RFI's products, services and delivery channels.

2.38 The inherent vulnerability of a product, service, or delivery channel is its utility and resulting attractiveness for the purposes of ML/TF, before applying any risk mitigation measures.

2.39 An RFI should assign inherent vulnerability risk ratings to each of its products, services and delivery channels. The more useful and attractive a particular product, service or delivery channel is to persons seeking to launder money or finance terrorism, the higher its inherent vulnerability risk rating should be.

2.40 Some higher risk products or services may include those that can be used to:

- Mask the origin or destination of funds;
- Obscure the true identity of an actual owner or beneficiary;
- Conduct business with higher-risk business segments, or in or with higher-risk jurisdictions;

- Carry out business for a third party; or
- Move funds to finance terrorist acts.

2.41 Delivery channels can significantly affect an RFI's assessment of risk. RFIs should consider the extent to which a particular business relationship or occasional transaction is carried out directly with a customer, remotely via mail, telephone, fax or the internet or through intermediaries or correspondent institutions.

2.42 Some higher risk delivery channels may include those that involve:

- Non face-to-face customer acceptance or transacting; or
- Third-party intermediaries, agents or brokers.

2.43 An RFI's risk ratings should differentiate those products, services and delivery channels that are inherently more vulnerable to ML/TF from those that are inherently less vulnerable. As with threat ratings, there are many ways to assign a risk rating to each product, service and delivery channel. One approach is to assign an inherent vulnerability risk rating of high, medium or low.

2.44 Customer risk ratings (threat) and inherent vulnerability risk ratings (vulnerability) should be combined to identify the inherent likelihood (likelihood) of a particular customer carrying out ML/TF through a particular combination of product, service and delivery channel. The table below illustrates one way to combine two separate ratings to produce a five-level or nine-level measure of the inherent likelihood that ML/TF will occur.

Customer Risk Rating	*High*	Medium 6	Medium-High 8	High 9
	Medium	Medium-Low 3	Medium 5	Medium-High 7
	Low	Low 1	Medium-Low 2	Medium 4
Inherent Likelihood of ML/TF Occurring		*Low*	*Medium*	*High*
		Inherent Vulnerability Rating		

2.45 RFIs should assign inherent likelihood risk ratings to each potential combination of various vulnerabilities. This involves overlaying the assessments associated with customers, products, services, delivery channels and geographic connections to assess the inherent likelihood of ML/TF occurring in connection with a particular business relationship or occasional transaction.

2.46 For example, the inherent risk rating assigned to a small domestic wire transfer initiated by a resident individual in a face-to-face transaction at a bank branch will likely differ from the inherent risk rating assigned to a large international wire transfer initiated by a non-resident corporation via the internet from a third jurisdiction.

Third party service providers

2.47 Prior to entering into any outsourcing or reliance relationship, an RFI should assess the risks of involving such a third party service provider in AML/ATF compliance matters for which the RFI is ultimately responsible. The risks identified should be factored into the decision whether or not to enter into the relationship, and into the risk ratings for any customers, products, services and transactions affected by the relationship. For additional information on assessing the risks associated with third party service providers, see paragraphs 5.130 through 5.139, 5.153 through 5.157 and 5.165.

Geographic connections

2.48 When assigning risk ratings, RFIs should be cognisant of the geographic connections of their customers, services, products, transactions and delivery channels and should consider whether there is a material connection to any high-risk jurisdiction. A material connection may include:

- A customer who is a resident in, or citizen of, a high-risk jurisdiction;
- A transaction to or from a high-risk jurisdiction;
- A non face-to-face transaction initiated from a high-risk jurisdiction; or
- A transaction linked to business in or through a high-risk jurisdiction.

2.49 RFIs should also be cognisant of any sanctions regimes in place. See **Chapter 6: Sanctions**.

II. Establish risk tolerance

2.50 Risk tolerance is the amount of risk an RFI decides to accept in pursuit of its business goals.

2.51 Nothing in the Acts or Regulations prevents an RFI from deliberately choosing to have a high risk tolerance. An RFI must, however, ensure that it has the capacity and expertise to apply risk mitigation measures that are commensurate with the risks it faces, and that it does effectively apply those measures.

2.52 An RFI's risk tolerance impacts its decisions about risk mitigation measures. If, for example, an RFI determines that the risks associated with a particular type of customer exceed its risk tolerance, it may decide not to accept or maintain that particular type of customer. Conversely, if the risks associated with a particular type of customer are within the bounds of an RFI's risk tolerance, the RFI must ensure that the risk mitigation measures it applies are commensurate with the risks associated with the customer.

2.53 An RFI with a large number of high-risk customer-product combinations may have the capacity and experience to effectively manage all of its risks, and thus may choose to have a higher risk tolerance. By contrast, an RFI with a vast majority of medium-risk customer-product combinations, and only one higher-risk customer-product combination, may not be able or willing to dedicate the compliance resources necessary to effectively manage the higher risk. As a result, such an RFI may establish a correspondingly lower risk tolerance and choose not to accept or maintain higher-risk customer-product combinations.

2.54 Each RFI should consider:

- The risks it is willing to accept;
- The risks it is unwilling to accept;
- The risks that will be sent to senior management for a decision; and
- Whether the RFI has sufficient capacity and expertise to effectively manage the risks it decides to accept.

2.55 In establishing its risk tolerance, an RFI should consider the following consequences of an AML/ATF compliance failure:

- Legal consequences;
- Regulatory consequences;
- Financial consequences; and
- Reputational consequences.

2.56 One way to visualise risk tolerance is to combine the likelihood risk rating assigned to a particular combination of customer, product, service and delivery channel with a consequence rating of high, medium or low.

2.57 It is important to note that an RFI may wish to establish its risk tolerance on the basis of its inherent likelihood, residual likelihood or both. Thus, the likelihood rating used to visualise risk tolerance may be one or both of:

- The inherent likelihood rating, which is based on a combination of customer risk and inherent vulnerability (See Step I of the business risk assessment cycle, in paragraphs 2.25 through 2.49); or
- The residual vulnerability rating, which is based on a combination of customer risk and residual vulnerability (See Step IV of the business risk assessment cycle, in paragraphs 2.67 through 2.74).

2.58 The table below illustrates one way to combine a five-level measure of likelihood with a three-level consequence rating. The result is a seven-level or fifteen-level measure of total risk.

Consequence	*High*	Medium-Low 6 (Acceptable Risk)	Medium 9 (Acceptable Risk)	Medium-High 12 (Acceptable Risk)	High 14 (Unacceptable Risk)	Very High 15 (Unacceptable Risk)
	Medium	Low 3 (Acceptable Risk)	Medium-Low 5 (Acceptable Risk)	Medium 8 (Acceptable Risk)	Medium-High 11 (Acceptable Risk)	High 13 (Unacceptable Risk)
	Low	Very Low 1 (Acceptable Risk)	Low 2 (Acceptable Risk)	Medium-Low 4 (Acceptable Risk)	Medium 7 (Acceptable Risk)	Medium-High 10 (Acceptable Risk)
Total Risk (With Risk Tolerance Notations)		*Low*	*Medium-Low*	*Medium*	*Medium-High*	*High*
		ML/TF Likelihood *(Threat * Vulnerability)*				

2.59 The above designations of "acceptable risk" and "unacceptable" risk are examples only. Each RFI should make its own determinations concerning the levels of risk if finds acceptable and unacceptable.

III. Establish risk mitigation measures

2.60 An RFI must develop and document appropriate policies, procedures and controls to minimise and manage the risks it has assessed.

2.61 The policies, procedures and controls must be commensurate with the risks it has identified.

2.62 The higher the risk an RFI faces from any particular combination of customer, product, service, transaction, delivery channel or geographic connection, the stronger and/or more numerous the mitigation measures must be.

2.63 Examples of risk mitigation measures include:

- Tailoring customer identification and verification requirements to the risks posed by particular customers, products and combinations of both;
- Tailoring the scope and frequency of ongoing monitoring to the risks associated with particular customers, products and combinations of both;
- The establishment of norms for transactions and conduct, and procedures to identify and scrutinise persons or activities that fall outside of those norms;
- Setting transaction limits for higher-risk customers or products;
- Requiring senior management approval for higher-risk transactions;
- Requiring additional information to be collected and reviewed before authorising any transaction involving a higher-risk customer or jurisdiction;
- Providing regular training to employees as regards particular risks identified, and the proper procedures for managing those risks;
- Not accepting customers, products, services, transactions or third party service providers presenting risks higher than an RFI's risk tolerance.

2.64 Although RFIs should target compliance resources toward higher-risk situations, they must also continue to apply risk mitigation measures to standard- and lower-risk situations, commensurate with the risks identified. The fact that a customer or transaction is assessed as being lower risk does not mean the customer or transaction is not involved in ML/TF. Employees should remain vigilant and apply reason and experience at all times when designing and applying risk mitigation measures.

2.65 For additional information regarding risk-based CDD measures, including enhanced CDD measures, see **Chapter 5: Non-Standard Customer Due Diligence Measures**.

2.66 For additional information regarding the use of the risk-based approach for the purposes of establishing norms and ongoing monitoring, see **Chapter 7: On-going Monitoring**.

IV. Evaluate residual risks

2.67 Residual risk is the risk remaining after taking into consideration the risk mitigation measures an RFI has designed and documented.

2.68 Regardless of the strength of an RFI's risk mitigation methods, there will always be some residual ML/TF risk, which RFIs must manage.

2.69 RFIs should determine the level of residual risk for each combination of customer, product, service, transaction, delivery channel and geographic connection to which an inherent likelihood risk rating was assigned.

2.70 In combining the customer risk ratings and vulnerability risk ratings to ascertain the likelihood of ML/TF occurring, the vulnerability rating assigned should take into account all of the risk mitigation measures established and documented by the RFI. Each RFI should consider the degree to which its risk mitigation measures affect its risk assessments, and whether the measures are appropriately mitigating the risks the RFI faces.

2.71 The table below illustrates one way to combine a customer risk rating with a residual vulnerability rating to produce a five-level or nine-level measure of the residual likelihood that ML/TF will occur.

Customer Risk Rating	*High*	Medium 6	Medium-High 8	High 9
	Medium	Medium-Low 3	Medium 5	Medium-High 7
	Low	Low 1	Medium-Low 2	Medium 4
Residual Likelihood of ML/TF Occurring		*Low*	*Medium*	*High*
		Residual Vulnerability Rating		

2.72 Each RFI should ensure that its residual likelihood ratings, when combined with the legal, regulatory, financial and reputational consequences of a compliance failure, produce total

residual risk ratings that are in line with the RFI's risk tolerance. (See step II of the business risk assessment cycle, in paragraphs 2.50 through 2.59).

2.73 Where an RFI finds that the level of residual risk exceeds its risk tolerance, or that its risk mitigation measures do not adequately mitigate high-risk customers or business relationships, the RFI should increase the level, strength or quantity of its risk mitigation methods.

2.74 RFIs should be cognisant of the risk associated with accepting a higher-risk customer for a lower-risk product or service where it may be possible for the customer to later migrate to a higher-risk product or service.

V. Implement risk mitigation measures

2.75 After establishing its risk mitigation policies, procedures and controls, an RFI should implement those policies, procedures and controls as part of its day-to-day activities.

2.76 An RFI's policies, procedures and controls should be well-documented, with the relevant information available to employees and senior management, to ensure consistent implementation.

2.77 At a minimum, the RFI should document its policies, procedures and controls for:

- Risk assessment;
- Customer due diligence;
- Special measures for higher risks;
- Ongoing monitoring;
- Detecting and reporting suspicious activity;
- Record-keeping and retention; and
- Reliance and outsourcing relationships.

2.78 It is the responsibility of senior management to ensure that the RFI's risk-based policies, procedures and controls are clear and complete, and that employee training and awareness reflects the risks and needs identified through the risk assessment process.

VI. Monitor and review risks

2.79 The assessment of ML/TF risk is not a static exercise. Risks that have been identified may change or evolve over time due to any number of factors, including shifts in customer conduct, the development of new technologies, and changes in the marketplace, including

the rise of new threats. Each RFI should re-evaluate and update its risk-based approach on a regular basis, and each time the risk factors change.

2.80 RFIs should ensure that their compliance programme is reviewed to assess the implications of:

- New products, services and delivery channels;
- New ML/TF trends or typologies;
- New regulatory guidance;
- Changes in customer portfolios or conduct;
- Changes in products, services and delivery channels;
- Changes in business practices; and
- Changes in the law.

2.81 All aspects of an RFI's AML/ATF policies, procedures and controls should be fully reviewed as part of the RFI's independent AML/ATF audit. See paragraphs 1.75 through 1.79.

2.82 As noted in paragraph 1.75, the AML/ATF independent audit should be conducted at least once per year, and more frequently when senior management has become aware of any gap or weakness in the RFI's AML/ATF policies, procedures or controls, or when senior management deems necessary due to the RFI's assessment of the changing risks it faces.

2.83 During the independent audit, an RFI should test the effectiveness of its AML/ATF policies, procedures and controls. Examples of testing methods that may be considered include:

- Sample testing business relationship activity to determine whether actual activity is consistent with anticipated activity;
- Sample test whether unusual activity was appropriately reviewed and reported;
- Sample test customer identification and verification information to ensure it meets the requirements of the RFI's policies, procedures and controls;
- Sample test the willingness and ability of any third parties holding CDD verification information to provide that information upon request;
- Sample test whether risk assessment ratings have been assigned to all customers, including introduced customers, and the adequacy of those ratings;
- Sample test the knowledge of relevant employees and senior management.

2.84 The results of each audit should be used to guide any improvements that the AML/ATF policies, procedures and controls require.

CHAPTER 3 - OVERVIEW OF CUSTOMER DUE DILIGENCE

Introduction

3.1 This chapter, and the subsequent **Chapters 4 and 5**, provide guidance on the obligations of RFIs to know their customers.

3.2 Standard customer due diligence (CDD) measures are governed primarily by Regulations 5, 6, 8 and 9. Simplified and enhanced CDD measures are governed primarily by Regulations 10 and 11.

What is customer due diligence?

3.3 CDD measures that must be carried out involve:

- Identifying the customer and verifying the customer's identity;
- Identifying the beneficial owner, verifying the beneficial owner's identity, and, where relevant, understanding the ownership and control structure of the customer; and
- Understanding the purpose and intended nature of the business relationship.

3.4 The extent of CDD measures must be determined using a risk-based approach. Higher-risk situations require the application of enhanced due diligence (EDD) measures. Lower-risk situations may be eligible for the application of simplified due diligence (SDD) measures.

3.5 RFIs must be able to demonstrate to the BMA that the extent of their CDD measures and monitoring is appropriate in view of the risks of ML/TF.

What is on-going monitoring?

3.6 RFIs must conduct on-going monitoring of the business relationship with each customer. On-going monitoring of a business relationship means:

- Investigating transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the RFI's knowledge of the customer and the customer's business and risk profile;
- Investigating the background and purpose of all complex or unusually large transactions, and unusual patterns of transactions which have no apparent economic or lawful purpose and recording in writing the findings of the investigation; and
- Reviewing existing documents, data and information to ensure that they are relevant, sufficient, and up-to-date for the purpose of applying CDD measures.

Why is it necessary to apply CDD measures and on-going monitoring?

3.7 The CDD and on-going monitoring obligations under the Regulations are designed to make it more difficult for RFIs to be used for money laundering or terrorist financing.

3.8 RFIs need to know the identities of their customers in order to guard against impersonation and other types of fraud, and to avoid committing offences under the POCA and the ATFA relating to ML/TF.

3.9 Carrying out CDD and on-going monitoring allow RFIs to:

- Be reasonably satisfied that customers are who they say they are;
- Know whether a customer is acting on behalf of another;
- Be aware of changes to the customer's risk profile;
- Identify any legal barriers (e.g. sanctions) to providing the product or service requested;
- Maintain a sound basis for identifying, limiting and controlling risk exposure of assets and liabilities; and
- Assist law enforcement by providing information on customers or activities being investigated.

3.10 These guidance notes describe a minimum level of acceptable CDD and on-going monitoring measures. In practice, RFIs often require additional information for the purposes of managing risks and providing products and services.

Timing of customer due diligence measures

3.11 An RFI must apply CDD measures when it:

- Establishes a business relationship;
- Carries out an occasional transaction in an amount of $15,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked, or carries out any wire transfer in an amount of $1,000 or more;
- Suspects money laundering or terrorist financing; or
- Doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

3.12 General rule – without exception, RFIs should always identify the customer and any beneficial owners, the purpose and intended nature of the business relationship, and, where

required, the source of funds before the establishment of a business relationship or the carrying out of an occasional transaction.

3.13 Subject to the exceptions referred to below, RFIs must also verify the identity of the customer and any beneficial owners before the establishment of a business relationship or the carrying out of an occasional transaction.

3.14 Exception for life insurance – the identification and verification of the customer of a life insurance policy must be completed before the establishment of the business relationship. However, verification of the identity of the beneficiary under the policy may take place after the business relationship has been established provided that verification takes place at or before the time of payout or at or before the time the beneficiary exercises any right vested under the policy.

3.15 Exception where essential to avoid interrupting normal business – on an exceptional basis, and only where the risk of money laundering and terrorism financing has been assessed as low, RFIs may verify the identity of the customer and any beneficial owners during the establishment of a business relationship, provided that the following safeguards are put in place:

- Ensuring that the exception is essential to avoid interrupting normal business;
- Establishing that there is little risk of money laundering or terrorism financing occurring and that any ML/TF risk is effectively managed;
- Completing the verification as soon as practicable after the initial contact;
- Ensuring that the business relationship is not closed prior to efforts to complete verification;
- Ensuring that funds received are not passed to third parties;
- Imposing, using a risk-based approach, limits on the number, types and/or amount of transactions that may be carried out prior to the completion of verification; and
- Monitoring, using a risk-based approach, by senior management of the first and each subsequent transaction until verification has been completed.

3.16 This exception may pertain to low-risk types of non-face-to-face business and high-speed securities transactions through a recognized stock exchange.

3.17 Because it takes time to form a trust, the time required for trust service providers to verify identify is not considered interruptive of normal business, and, as a result, this exception is not available to those service providers.

3.18 RFIs must satisfy themselves that the primary motive for the use of this exception is not for the circumvention of CDD procedures.

3.19 Where there is suspicion of money laundering or terrorist financing, this exception is not available.

3.20 Where a new business relationship is assessed as posing a higher risk, this exception is not available and enhanced due diligence is required.

Keeping information up to date

3.21 RFIs must review the documents, data and information they hold in relation to a customer to ensure that the records are up-to-date, adequate, and relevant to the business relationship or transaction. Once an RFI has verified the identity of a customer and any beneficial owners, it should re-verify where:

- Doubts exist as to the veracity or adequacy of the evidence previously obtained for the purposes of identifying and verifying the customer and any beneficial owners;
- There is suspicion of money laundering or terrorist financing in relation to the customer;
- The customer's activities are inconsistent with the RFI's understanding of the purpose and intended nature of the business relationship;
- There is a material increase in the risk rating assigned to the customer, or to the products, services, delivery channels, or geographic connections with which the customer engages;
- Other trigger events, such as an existing customer applying to open a new account or establish a new relationship, prompt an RFI to seek appropriate evidence.

Acquisition of one AML/ATF regulated financial institution, or a portfolio of customers, by another

3.22 Where a RFI acquires an AML/ATF regulated financial institution with established customers, or a portfolio or block of customers, the acquiring RFI should undertake enquiries on the granting RFI sufficient to establish the level and the appropriateness of the identification and verification data held in relation to the customers to be acquired.

3.23 An RFI may rely on the information and documentation previously obtained by the granting RFI, provided that:

- The granting RFI is an AML/ATF regulated financial institution within the meaning of Regulation 10(2);

- The acquiring RFI has assessed, through the use of sample testing and any other methods deemed reasonable and comprehensive, that the CDD policies, procedures and controls exercised by the granting RFI were satisfactorily applied; and
- The acquiring RFI has obtained from the granting RFI the CDD information and verification documentation for each customer to be acquired.

3.24 The acquiring RFI should carry out verification of identity as soon as practicable, in accordance with the acquiring RFI's requirements for customers opening accounts, where any of the following occurs:

- The sample testing shows that the customer identification and verification procedures previously undertaken by the granting RFI were not carried out to an appropriate standard; or
- The granting RFI's CDD policies, procedures or controls cannot be checked; or
- The customer records are not made available and accessible to the acquiring RFI.

Customers with whom RFIs had a business relationship on 1st January 2009

3.25 RFIs must take steps to ensure that they hold appropriate CDD information with respect to business relationships established before the 1st January 2009. Appropriate CDD information means information sufficient for the RFI to meet the current standard of applying CDD measures using the risk-based approach.

3.26 Each RFI must assess the risk of its own customer base, including the extent and nature of the CDD information held and whether any additional documentation or information may be required for existing customers. The requirement to conduct on-going monitoring of the business relationship with each customer extends to existing customers and requires RFIs to review existing documents, data and information to ensure that they are relevant, sufficient, and up-to-date for the purpose of applying the current standard of CDD measures.

3.27 RFIs must ensure that their policies, procedures and controls in respect of existing customers are appropriate and ensure that:

- The risks associated with their customer base are assessed;
- The identity of their customers, and any beneficial owners, is obtained and verified;
- The purpose and intended nature of the business relationship are understood; and
- The level of CDD is appropriate to the assessed risk of each business relationship.

3.28 Where a business relationship has been identified as a high-risk relationship, enhanced CDD is required.

3.29 RFIs that have not verified the identity of existing customers and any related beneficial owners, or that do not understand the purpose or intended nature of any business relationship are exposing themselves to the possibility of action for breach of the Regulations.

3.30 RFIs should take the necessary action to remedy any identified deficiencies and be satisfied that CDD information appropriate to the assessed risk is held in respect of each business relationship.

Requirement to cease transactions

3.31 Verification of identity of any beneficial owners, and, where applicable, the purpose and intended nature of the business relationship, once begun, should be pursued through to conclusion as soon as practicable.

3.32 If a prospective customer does not pursue an application for business, or if for any other reason an RFI is unable to apply CDD measures in relation to a customer, in accordance with Regulation 9, the RFI must:

- In the case of a proposed business relationship or transaction, not establish that business relationship and not carry out that occasional transaction with or on behalf of the customer;
- In the case of an existing business relationship, terminate that business relationship with the customer; and
- Consider making a report to the Financial Intelligence Agency, in accordance with its obligations under POCA and the ATFA.

3.33 Where the immediate termination of a business relationship is impracticable due to contractual or legal reasons outside of the control of the RFI, the RFI must ensure that the risk is managed and mitigated effectively until such time as termination of the relationship is practicable.

3.34 Where funds have already been received and the RFI concludes that the circumstances support the making of a report to the Financial Intelligence Agency, the RFI must retain the funds until a competent authority has given consent for the return of the funds to the original source from which they came.

3.35 Where funds have already been received and the RFI concludes that there are no grounds for making a report to the Financial Intelligence Agency, it will need to determine whether to

retain the funds while seeking other ways of being reasonably satisfied as to the customer's identity, or whether to return the funds to the original source from which they came. Returning the funds in such circumstances is part of the process of terminating the business relationship; it is closing the account, rather than carrying out a transaction with or on behalf of the customer.

Shell banks and anonymous accounts

3.36 RFIs must not enter into, or continue, a correspondent banking relationship with a shell bank. RFIs must take appropriate measures to ensure that they do not enter into or continue a correspondent banking relationship with a bank that is known to permit its accounts to be used by a shell bank.

3.37 A shell bank is an entity incorporated in a jurisdiction where it has no physical presence involving meaningful decision-making and management, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.

3.38 RFIs carrying on business in Bermuda must not establish any anonymous account or any anonymous passbook for any new or existing customer. All RFIs carrying on business in Bermuda must immediately apply CDD measures to any existing anonymous accounts and passbooks and must not permit such accounts or passbooks to be used in any way prior to the satisfactory application of all appropriate CDD measures. The satisfactory application of CDD measures will effectively remove the anonymity of any account or passbook.

3.39 RFIs should pay special attention to any money laundering or terrorist financing risks that may arise from products, services, transactions, delivery channels, or geographic connections that may favour anonymity. RFIs should take appropriate measures, where risk dictates, to prevent their use for money laundering or terrorist financing purposes.

CHAPTER 4 - STANDARD CUSTOMER DUE DILIGENCE MEASURES

Nature and purpose of proposed business relationship

4.1 An RFI must understand the purpose and intended nature of each proposed business relationship or transaction. In some instances the purpose and intended nature of a proposed business relationship may appear self-evident. Nonetheless, an RFI must obtain information that enables it to categorise the nature, purpose, size and complexity of the business relationship, such that it can be effectively monitored.

4.2 Where an occasional transaction outside of an on-going business relationship is small and not considered high risk, information based on a brief conversation with, or knowledge of, an individual customer may be sufficient.

4.3 Where an occasional transaction or business relationship involves larger sums or is of a commercial nature, and particularly where the customer is a legal person or legal arrangement, formal CDD measures should be applied and recorded in accordance with these guidance notes.

4.4 To obtain an understanding sufficient to monitor the business relationship, an RFI may need to collect additional information, including, but not limited to:

- The anticipated type, volume, value and nature of the activity that is likely to be undertaken through the relationship;
- The expected source and origin of the funds to be used in the relationship (particularly the source of wealth within a private banking or wealth management relationship, or in a relationship involving a trust company or corporate service provider);
- The customer's current and past addresses and geographic areas of operation;
- Copies of recent and current financial statements; and
- Documentation evidencing the relationships between signatories and underlying beneficial owners.

Customer identification and verification of private individuals

4.5 An RFI identifies a customer by obtaining a range of information about him. An RFI verifies the identity of a customer by comparing information obtained from the customer against documents, data or information obtained from reliable and independent sources.

4.6 The meaning of the term 'customer' should be inferred from the definitions of 'business relationship' and 'occasional transaction', the context in which it is used in the Regulations and its everyday dictionary meaning.

4.7 A customer is generally the private individual or individuals with whom a business relationship is established, or for whom a transaction is carried out.

4.8 The Regulations define a 'business relationship' as a business, professional or commercial relationship between an RFI and a customer, which, at the time contact is first made, the RFI expects to have an element of duration. A business relationship is also formed where the expectation of duration is not initially present, but develops over time. A relationship need not involve the RFI in an actual transaction; giving advice may often constitute the establishment of a business relationship.

4.9 The term 'occasional transaction' means a transaction carried out outside of a business relationship, amounting to $15,000 or more, whether the transaction is carried out in a single operation or several operations that appear to be linked. The term 'occasional transaction' also means any wire transfer carried out in an amount of $1,000 or more.

4.10 Transactions separated by an interval of three months or more need not be treated as linked, provided there is no evidence of a link and the transactions do not otherwise give rise to a business relationship.

Private individuals as beneficial owners

4.11 A beneficial owner is normally an individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. In respect of customers who are private individuals, the customer himself is the beneficial owner, unless there are features of the transaction or surrounding circumstances that indicate otherwise.

4.12 Where there is reason to believe that a person is not acting on his own behalf, an RFI should make appropriate enquiries to identify and verify the customer and beneficial owner. Where a private individual is fronting for another private individual who is the beneficial owner, the RFI should obtain the same information about that beneficial owner as it would for a customer. For further guidance regarding a person acting under power of attorney or as an executor or personal representative, see paragraphs 4.45 to 4.47.

Characteristics and evidence of identity

4.13 For the purposes of CDD, an individual's identity comprises information that cannot change (e.g., date and place of birth) and information that may change and accumulate over time (e.g. name, addresses, family circumstances, employment, positions of authority and physical appearance). To the extent that information concerning identity is available online or in electronic databases, such information may be referred to as an 'electronic footprint'.

4.14 Identifying customers and verifying identity is generally a cumulative process, which requires more than one document or data source to verify all of the necessary components. RFIs should be prepared to accept and verify a range of documents and data.

4.15 An RFI must utilise a risk-based approach to determine the extent of identity information or evidence it requests and verifies. In making its determinations, an RFI should take into account factors such as:

- The nature of the product or service sought by the customer;
- The nature of any other products or services to which the customer may migrate without further identity verification;
- The nature and length of any existing or previous relationship between the customer and the RFI;
- The nature and extent of any assurances from other RFIs that may be relied upon; and
- Whether the customer is physically present.

4.16 Evidence of identity may be in documentary or electronic form. An appropriate record of the steps taken, and copies or records of the evidence obtained to identify the customer, must be kept as per the record-keeping portion of this guidance.

Documentary evidence

4.17 Documentation purporting to offer evidence of identity may emanate from a number of sources. Documents differ in their integrity, reliability and independence. Some documents are issued after due diligence on an individual's identity has been undertaken; others are issued upon request, without any such checks being carried out. There is a broad hierarchy of documents:

- First and foremost, certain documents issued by government departments and agencies, or by a court; then
- Certain documents issued by other public sector bodies or local authorities; then
- Certain documents issued by regulated RFIs in the financial services sector; then
- Documents issued by other RFIs subject to the Regulations, or to equivalent legislation; then
- Documents issued by other organisations.

4.18 Wherever possible, RFIs should seek documents at the highest level of the hierarchy. To provide the highest level of confidence in an individual's identity, an identification document should contain a photo of the individual, and it should be issued by a government department or agency that is known to carry out due diligence prior to issuing the document.

4.19 Non-government issued documentary evidence complementing identity should normally be accepted only if it originates from a public sector body, or if it is supplemented by an RFI's documented knowledge of the individual.

4.20 Where business is conducted face-to-face, RFIs should see and make copies of the originals of any documents involved in the verification. Copies of documents should be verified as true copies of the original documents. Customers should be discouraged from sending original valuable documents by post.

4.21 RFIs should give consideration as to whether any document relied upon is forged. Where suspicion arises in relation to any document offered, RFIs should take practical and proportionate steps to establish whether the document offered is valid, whether it has been reported as lost or stolen and whether any reporting requirements have been implicated.

4.22 RFIs may wish to use commercial software to assist in verifying the validity of machine-readable passports.

4.23 Where a document is provided in a language other than English, the RFI should obtain an English translation of the document. The RFI should be satisfied that the translated document is a fair and true representation of the original document.

Standard identification requirements for private individuals

4.24 Subject to situations in which simplified due diligence is applicable, an RFI should obtain the following information in relation to each private individual:

- Full legal name, any former names (e.g. maiden name) and other names used;
- Principal residential address;
- Date of birth;
- Place of birth;
- Nationality;
- Gender; and
- A personal identification number or other unique identifier contained in a valid government-issued document.

4.25 On a risk-sensitive basis, the RFI should also collect the following information:

- Occupation and name of employer/source of income; and
- Details concerning any public or high-profile positions held.

Documentary verification

4.26 Where seeking to verify identity using documents, an RFI's assessment should be based upon:

Either a valid government issued document, such as a passport, national identity card, or driving licence that incorporates the individual's full legal name and photograph and at least one of the following:

- Principal residential address;
- Date of birth

or a government issued document lacking a photograph, such as a birth certificate, which incorporates the individual's full legal name, **supported by one or more additional documents** which incorporate the individual's full legal name and cumulatively provide both of the following:

- Principal residential address; and
- Date of birth.

4.27 Where any additional document is used for the purposes of verification, the document should be government issued or issued by a judicial authority, a public sector authority, a utility company or another RFI in Bermuda or in a jurisdiction that imposes equivalent AML/ATF requirements. Examples of other acceptable supporting documents include:

- Instrument of a court appointment (such as liquidator, or grant of probate);
- Current land tax demand letter, bill, or statement;
- Current bank statements, or credit/debit card statements, issued by a Bermuda RFI or an institution in a jurisdiction that imposes equivalent AML/ATF requirements, provided the document is not printed from the Internet;
- Utility bill.

4.28 The examples of other documents are intended to support the verification of a customer's address.

4.29 Where an employee of the RFI has visited the individual at his or her principal residential address, a record of the visit may constitute a second document corroborating that the individual lives at the address.

Electronic verification

4.30 Electronic databases can provide a wide range of confirmatory material without involving the customer.

4.31 RFIs may assess the degree to which they are satisfied as to a customer's identity by corroborating information supplied by the customer against information in an electronic database. The greater the depth, breadth and quality of the data held on a customer in a particular electronic database, the more useful the electronic database will be for the purposes of corroborating the information supplied by a customer.

4.32 A number of electronic databases provide online access to RFIs seeking a primary interface for the purposes of verifying identity. Electronic databases may provide access to both positive and negative information concerning an individual.

4.33 Positive information concerning, for example, an individual's name, address and date of birth, may be useful in confirming that an individual exists.

4.34 Negative information, such as lists of individuals who are deceased, subject to sanctions or known to have committed fraud, may be useful in assessing the risks associated with a proposed transaction or business relationship, including the risks of impersonation fraud.

4.35 For an electronic check to provide satisfactory confirmation of identity, it must use data from multiple sources and across time, or incorporate qualitative checks that assess the strength of the information supplied. An electronic search that accesses data from a single source (e.g. a single search of a government registry) is not normally sufficient to verify identity.

4.36 Before using a commercial agency for electronic verification, RFIs should be satisfied that information supplied by the data provider is sufficiently extensive, reliable and accurate. This judgement may be assisted by considering whether the provider meets all the following criteria:

- It is registered with a data protection agency in a jurisdiction such as the European Economic Area that imposes AML/ATF requirements equivalent to those in Bermuda;
- It uses multiple positive information sources that can be called upon to link a customer to both current and previous circumstances;

- It accesses multiple negative information sources, such as databases relating to deceased persons, sanctions, money laundering, terrorist financing, and identity fraud; and
- It has transparent processes that enable the RFI to understand what checks were carried out, what the results of these checks were and how each check performed affects the level of certainty as to the identity of a person or entity.

4.37 In addition, an electronic database should have processes that allow RFIs to meet their obligations to capture and store the information used to verify an identity.

4.38 For an RFI using an electronic database to be reasonably satisfied that a customer is who he says he is, the standard level of confirmation is:

- One match on an individual's full name and current address; and
- A second match on an individual's full name and either his current address or his date of birth.

4.39 Where circumstances give rise to concern or doubt, RFIs should use a risk-based approach to determine an appropriately higher level of confirmation.

4.40 Electronic databases may display verification results according to the number of documents searched, a scoring mechanism or some other means. RFIs should ensure that they understand the basis of the system in use, in order to be satisfied that the sources of the underlying data reflect this guidance and cumulatively meet the required level of confirmation set out in paragraph 4.38.

4.41 To mitigate the risk of impersonation fraud, RFIs should either verify with the customer additional aspects of his identity that are held electronically, or follow the guidance in paragraph 4.42.

Mitigation of impersonation fraud

4.42 Where an RFI cannot obtain identification documents that bear a photograph of the customer and match those documents against the customer in a face-to-face setting, a RFI should apply additional verification measures to manage the risk of impersonation fraud. The additional measures may consist of robust anti-fraud checks that the RFI routinely undertakes as part of its existing procedures, or may include a combination of:

- Requiring the first payment to be carried out through an account in the customer's name with a regulated financial institution in Bermuda or a jurisdiction that imposes equivalent AML/ATF requirements;

- Verifying additional aspects of the customer's identity, or of his electronic 'footprint' (see paragraph 4.13);
- Requiring copy documents to be certified by an appropriate person;
- Telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise), or a "welcome call" to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;
- Communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, is required to be returned completed or acknowledged without alteration);
- Internet sign-on following verification procedures where the customer uses security codes, tokens or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address; and
- Other reasonable card or account activation procedures.

Variation from the standard

4.43 The standard identification requirement for documentary and electronic approaches is likely to be sufficient for most situations. In some situations, however, variations from the standard are permitted or required.

4.44 Where an individual or the product, service, delivery channel or geographic counterparty with which he transacts is assessed as presenting a higher risk for money laundering or terrorist financing, RFIs may require additional identity information and additional verification matches.

4.45 When a person deals with assets under a power of attorney, that person is also a customer of the RFI. Consequently, the identity of holders of powers of attorney should be verified.

4.46 Where the donor of a power of attorney is of legal age and sound mind, and therefore has control, he remains the owner of the funds, and remains the customer. Other than where he is an existing customer of the RFI, therefore, his identity must be verified.

4.47 In circumstances where the donor of a power of attorney is not of legal age and sound mind, the donor remains or becomes a beneficial owner and his identity should be verified.

4.48 During the course of administering the estate of a deceased person, the beneficial owner is the executor or administrator of the deceased person.

Receipt of funds as evidence of identity

4.49 Under certain conditions, where the ML/TF risk in a product or service is assessed to be at its lowest, the receipt of funds from an account which is in the sole or joint name of the individual may satisfy the standard identification requirement, provided that:

- All initial and future funds are received from a Bermuda RFI or an institution in a jurisdiction that imposes equivalent AML/ATF requirements;
- All initial and future funds come from an account in the sole or joint name of the customer or underlying principal;
- Payments are made solely to accounts in the customer's name (i.e., no third party payments are allowed);
- No payments are 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 the cash withdrawal are verified.

4.50 RFIs will need to be able to demonstrate why they considered it to be reasonable to have regard to the source of funds as evidence in a particular instance. RFIs 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 ML/TF.

4.51 Where a relationship has been established, and any of the conditions in paragraph 4.48 is no longer met, RFIs must then verify the identity of the customer and any underlying principals.

4.52 Where an RFI has reason to suspect the motives behind a particular transaction, or believes that a business relationship has been or is being structured to avoid the standard identification requirement, it should not permit the use of the receipt of funds as evidence of identity.

Customers who cannot provide the standard evidence

4.53 Some customers who are considered to be lower risk may be unable to provide the identification information described in paragraphs 4.26 to 4.27. Such customers may include, for example, certain low-income individuals, individuals with a legal, mental or physical inability to manage their affairs, or individuals dependent on the care of others,

such as the elderly, minors and prison inmates. In certain situations, such customers may also include students and other young persons.

4.54 In general, such customers are or were Bermuda residents.

4.55 In the case of the elderly and the incapacitated, the business relationship may be limited to the receipt of social security benefits; in the case of minors, the business relationship may be limited to periodic savings deposits linked to events such as birthdays or holidays. Such business relationships would appear to represent a less than standard risk of money laundering activity.

4.56 RFIs should adopt a broad view of financial inclusion and seek to ensure that, where lower-risk residents cannot reasonably be expected to produce standard evidence of identity, they are not unreasonably denied access to financial services.

4.57 Where standard documentation is not available, RFIs should seek alternative documentation to cumulatively provide assurance as to the identity of the customer. Examples of such alternative documentation include:

- A letter from the head of the household at which the individual resides confirming that the applicant lives at that address, setting out the relationship between the applicant and the head of household, together with evidence that the head of household resides at the address;
- A letter on appropriate business letterhead from a known nursing home or residential home for the elderly confirming residence of the applicant;
- A letter on appropriate business letterhead from a director or manager of a known Bermuda employer that confirms residence at a stated Bermuda address, and indicates the expected duration of employment;
- In the case of a student, a letter on appropriate letterhead from a principal of a known university or college that confirms residence at a stated address (the student's residential address in Bermuda should also be obtained); and
- In the case of a family member or guardian establishing an account in respect of a minor, the identity of the adult should be verified and the RFI should view a birth certificate or passport, and retain a copy.

4.58 In the limited circumstances described above, RFIs should require an employee of suitable seniority to undertake and document a review and sign-off procedure.

4.59 Using a risk-based approach, RFIs may consider placing limitations or restrictions on the types or volume of transactions permissible through a business relationship verified using alternative documentation. Regardless, RFIs should monitor business relationships for

activity inconsistent with the initial understanding of the purpose and intended nature of the business relationship.

4.60 RFIs offering financial services directed at the financially aware should consider whether any apparent inability to produce standard levels of identification evidence is consistent with the targeted market for these products.

Identification and verification of legal persons and other customers who are not private individuals

4.61 A customer that is not a private individual generally involves a number of individuals, such as directors, trustees, beneficial owners or other persons with an ownership interest or controlling interest. An RFI must therefore identify not only the customer itself, but also the individuals who comprise the customer and its relationship with the RFI.

4.62 At a minimum, for each customer that is not a private individual, RFIs must:

- Identify the customer and verify its identity;
- Gather information sufficient to understand the legal form, control structure and ownership structure of the customer;
- Gather information sufficient to understand the nature and purpose of the business relationship or transaction (see paragraphs 4.1 through 4.4);
- Identify the beneficial owners of the customer; and
- Identify and verify directors and other persons exercising control over the management of the customer or its relationship with the RFI.

4.63 RFIs should consider whether they have collected information sufficient to understand and dispel any doubt concerning:

- The anticipated type, volume, value, nature, location and complexity of the activity that is likely to be undertaken through the relationship;
- The customer's legal form, ownership structure and control structure;
- The identity of the private persons associated with the customer (particularly the beneficial owners and/or persons exercising control); and
- The relationships between persons exercising control and underlying beneficial owners.

4.64 RFIs must be satisfied that they know the customer, including its beneficial owners, and that they have identified, assessed and mitigated any money laundering or terrorist financing risks associated with the customer or its business relationship with the RFI.

4.65 RFIs must use a risk-based approach to determine the extent to which additional information needs to be collected and whether additional verification needs be carried out.

4.66 Verifications should be carried out on the basis of independent documentation checks or, where applicable, electronic databases. RFIs should bear in mind that information contained on an entity's internet website is generally not independently verified before being made publicly available.

4.67 Regarding evidence of ownership structure, control structure, authorisations and other powers, RFIs should obtain sight of and retain record of original documents. Where it is impractical or impossible to do so, RFIs should seek to obtain a copy certified by the company secretary, director, manager or equivalent officer or by another appropriate certifier.

4.68 When verifying the identity of private individuals associated with a customer, RFIs should use the same standards that apply to customers who are private individuals, as contained in paragraphs 4.5 through 4.60.

4.69 RFIs should take appropriate steps to avoid fraud due to impersonation, whether of a private person acting on behalf of a customer, or of a legal person or legal arrangement itself.

4.70 RFIs should verify that the customer has properly authorised each private individual that the RFI deals with. RFIs should identify and verify the identity of each such individual.

4.71 RFIs should ascertain the reason for the granting of any power of attorney or similar third party mandate that provides one or more otherwise unauthorised persons with the right to act on an entity's behalf. Where no reason is evident, or where the scope of the mandate granted is unnecessarily broad, RFIs should closely scrutinise both the instrument granting the mandate and the proposed transaction or business relationship. RFIs may wish to identify and verify additional information before determining whether to proceed.

4.72 In all cases, RFIs should obtain a copy of the original power of attorney or equivalent instrument and should verify the identity of each person to which a mandate has been granted.

4.73 RFIs should give consideration as to whether any document relied upon is forged. Where suspicion arises in relation to any document offered, RFIs should take practical and proportionate steps to establish whether the document offered is valid, whether it has been reported as lost or stolen, and whether a suspicious activity report must be filed.

4.74 Where a document is in a foreign language, RFIs should take appropriate steps to ensure that the document in fact provides the evidence sought.

Beneficial owner identification and verification for legal persons and other customers who are not private individuals

4.75 Irrespective of the geographic location of a customer, the complexity of a customer's structure or the means by which any business relationship is initiated, RFIs must know the identity of the persons who effectively control or own a customer. Limited exceptions to this fundamental rule are detailed in paragraph 4.95.

4.76 For the purposes of this guidance, beneficial owners are any persons, whether private individuals, legal persons or legal arrangements, that effectively control or own more than 25% of a customer's funds, assets or voting rights or, in the case of trusts or similar legal arrangements, on whose behalf a transaction is carried out. In the case of a corporate service provider, a beneficial owner is any person that effectively controls or owns more than 10% of the corporate service provider's customer's funds or assets. The meaning of 'control' and 'own' in this context should be interpreted broadly to comprise the capacity to:

- Manage funds, assets, accounts or investments without requiring further authorisation;
- Override internal procedures and control mechanisms;
- Derive benefit, whether presently or in the future;
- Exercise a specified interest, whether presently or in the future; and/or
- Add or remove beneficiaries, trustees or other persons associated with a customer.

4.77 At all times, RFIs should identify and take reasonable, risk based, measures to verify the private individuals who, either directly or indirectly via another individual, legal person or legal arrangement, ultimately control or own more than 25%, or, in the case of a corporate service provider, 10%, of a customer's funds or assets.

4.78 Where control or ownership is held by another legal person or legal arrangement, RFIs should take reasonable measures to identify and verify the private individuals who ultimately control or own that other legal person or legal arrangement.

4.79 Where a customer is a legal person administered by a corporate service provider, RFIs must identify the underlying beneficial owners, founders and any other beneficiaries of the legal person. Where the corporate service provider provides management services or corporate officers for the legal person, the client(s) paying the corporate service provider for those services or officers, together with any other persons on behalf of whom the corporate service provider is acting with regard to the legal person, must be identified.

4.80 In collecting identification information on all relevant private individuals, RFIs should ensure that the information collected is sufficient for the purposes of determining whether any higher risk persons are associated with the business relationship or transaction.

4.81 Where a customer seeks to authorise signatories who are not among the private individuals an RFI has previously identified, the RFI should collect information sufficient to determine whether the powers assigned to each signatory are significant and whether any higher risk persons are associated with the business relationship. Where a signatory's powers are significant, the identity of that signatory should be verified.

Legal persons and corporates

4.82 Legal persons, including corporates vary greatly in terms of size, complexity, activities undertaken and the degree to which their control and ownership structures are transparent. Corporates listed on an appointed stock exchange tend to be large, complex and, due to their public ownership, transparent. Privately held corporates may be of a range of sizes and complexity, but tend to be less transparent.

4.83 Regardless of a particular corporate's features, RFIs must use a risk based approach to determine whether there are legitimate commercial purposes for the size, structure and level of transparency of each customer and whether the customer or business relationship entails a heightened level of money laundering or terrorist financing risk.

4.84 In addition to the information required for all customers, RFIs must obtain the following identification information in relation to each corporate customer:

- Full name and any trade names;
- Date and place of incorporation, registration or establishment;
- Registered office address and, if different, mailing address;
- Address of principal place of business;
- Whether and where listed on an exchange;
- Official identification number (where applicable); and
- Name of regulator (where applicable).

4.85 For corporates not subject to paragraph 4.95, RFIs must also obtain identification information, in line with the guidance for private persons, and, where relevant, legal persons, for:

- All directors and other persons exercising control over management of the corporate;

- All persons who, directly or indirectly, ultimately own or control more than 25%, or, in the case of a corporate service provider, 10%, of the customer's property, shares or voting rights; and
- All other persons purporting to act on behalf of the corporate or by whom a binding obligation may be imposed on the corporate.

4.86 RFIs must verify the following in relation to each corporate customer:

- Full name;
- Date and place of incorporation, registration or establishment;
- Official identification number (where applicable);
- Current existence of the corporate;
- Ownership and control structures of the corporate;
- Subject to paragraphs 4.88 and 4.89, the identity of all directors, signatories and other persons exercising control over management of the corporate; and
- The identity of all other persons purporting to act on behalf of the corporate or by whom binding obligations may be imposed on the corporate.

4.87 In addition, and on the basis of an assessment of the ML/TF risks associated with a customer and its business relationship, RFIs must take reasonable measures to verify the identity of all persons who, directly or indirectly, own or control more than 25%, or in the case of a corporate service provider, 10%, of the customer's property, shares or voting rights.

4.88 Where the number of directors, signatories and other persons exercising control over management of the corporate is high, RFIs may use a risk-based approach to determine whose identity to verify. Where ML/TF risks are standard or low, RFIs should verify at least two of the relevant signatories and, where different, two directors or other individuals exercising significant control over management of the corporate. The individuals verified should be those the RFI expects to hold signatory powers for the purpose of operating an account or exchanging instructions. Where the money laundering or terrorist financing risks are high, or where a corporate may be seeking to avoid the application of certain CDD measures, the RFI may find it necessary to verify all directors and other individuals exercising significant control over the management of the corporate.

4.89 Where any individual associated with the corporate is assessed as high risk, or where a business relationship is assessed as higher risk for any reason, all directors and other individuals exercising control over management of the corporate must be verified.

4.90 The RFI should verify the existence, ownership and control structure of the corporate by:

- Confirming the corporate's listing on an appointed stock exchange;
- Confirming that the corporate is listed in the company registry of its place of formation and has not been dissolved, struck off, wound up or terminated;
- Obtaining and retaining the shareholder registry;
- Obtaining sight of and retaining record of the corporate's certificate of incorporation; and/or
- Obtaining sight of and retaining record of the corporate's memorandum and articles of association or equivalent constitutional documentation.

4.91 Regardless of the method(s) used, RFIS must verify all the required information.

4.92 Where RFIs are unable to complete verification using the methods contained in paragraph 4.90, where the size or complexity of a corporate is significant, or where a business relationship is otherwise assessed as higher risk, RFIs should consider the extent to which additional evidence is required. Additional means of verification may include:

- Reviewing an independently audited copy of the latest report and accounts;
- Reviewing the board resolution authorising the opening of the account and recording account signatories;
- Engaging a business information service or a reputable and known firm of lawyers or accountants to confirm the documents submitted;
- Utilising independent electronic databases; and
- Personally visiting the principal place of business.

4.93 An RFI should require corporate customers to notify it of any material change to:

- Persons who are directors, signatories, beneficial owners or other persons exercising control over management of the corporate;
- Powers or authorities assigned to such persons; and
- Other changes to the control or ownership structures of the customer.

4.94 It is the RFI's responsibility to maintain current information concerning the above, which includes updating their customer records when there are material changes, e.g. change in beneficial ownership (>25%).

<u>Companies listed on an appointed stock exchange</u>

4.95 Where a corporate customer's securities are listed on an appointed stock exchange, the corporate is publicly owned and RFIs may forego verifying the identity of the corporate's beneficial owners, provided that:

- The corporate is listed on an appointed stock exchange that is subject to Bermuda disclosure obligations or to disclosure obligations equivalent to those in Bermuda; or
- The corporate is a majority-owned and consolidated subsidiary of such a listed company.

4.96 Where a corporate is listed outside of Bermuda on a market that is not subject to disclosure obligations equivalent to those in Bermuda, RFIs must apply the verification requirements normally applicable to private and unlisted companies.

Bearer instruments

4.97 Legal persons and legal arrangements in some jurisdictions have the power to issue bearer shares, bearer warrants or other bearer negotiable instruments, hereafter referred to as 'bearer instruments', as evidence of title. RFIs should be cautious with such legal persons and legal arrangements as the use of bearer instruments may serve to obscure beneficial ownership.

4.98 In assessing the risks of a particular business relationship or transaction, RFIs should consider whether any legal person or arrangement that is a customer, beneficial owner or other associated person has issued or has the potential to issue bearer instruments.

4.99 RFIs should open accounts for legal persons or arrangements capable of issuing bearer instruments only where the holders and, where different, the ultimate beneficial owners are identified and verified.

4.100 Before proceeding with the business relationship or transaction, an RFI should ensure that all bearer instruments are held in secure custody by a Bermuda AML/ATF regulated financial institution or independent professional within the meaning of Regulation 14(2)(a) and (b). RFIs should obtain from the custodian an undertaking to notify the RFI prior to any release of a bearer instrument or any transfer of its ownership.

4.101 Where a potential or existing customer refuses to allow the immobilisation of all bearer instruments, RFIs should not proceed further with the business relationship or transaction, and must consider whether any reporting requirements have been implicated.

Trusts and other legal arrangements

4.102 A trust or other legal arrangement, such as an anstalt, stiftung, fiducie, treuhand, fideicomiso or foundation, can range in size, complexity and the degree to which its control and ownership structures are transparent.

4.103 The trustees of a trust generally exercise control over the trust property. In exceptional cases, another private individual may exercise control, such as a trust protector, or a settlor who retains significant powers over the trust property.

4.104 Regardless of a particular legal arrangement's features, RFIs must use a risk based approach to determine whether the customer and business relationship are legitimate and whether a request for facilities entails any money laundering or terrorist financing risk.

4.105 Most often, a trust or similar legal arrangement has no legal personality. In such cases, trustees or equivalent persons enter into the business relationship with the RFI, in their capacity as regards the particular trust or legal arrangement.

Obtaining identification information

4.106 In addition to the information required for all customers, RFIs must obtain the following identification information in relation to each customer that is a trust or other legal arrangement:

- Full name of the trust or other legal arrangement;
- Date and place of establishment;
- Registered address and, if different, mailing address;
- Legal form, nature and purpose (e.g., discretionary, testamentary, bare);
- Control and ownership structures; and
- Official identification number (where applicable).

4.107 In line with the guidance for private individuals and legal persons, RFIs must also obtain identification information for the following persons:

- Any donors, settlors, grantors or other persons making the arrangement;
- All trustees or other persons controlling or having power to direct the activities of the applicant;
- Any persons whose wishes the trustees or equivalent persons may be expected to take into account;
- Any persons purporting to act on behalf of a trustee or equivalent person; and
- Any other parties, including protectors and enforcers.

4.108 In addition, and in line with the guidance for private individuals and legal persons, RFIs must obtain identification information for all known beneficiaries at the time of disbursement. Known beneficiaries of trusts and other legal arrangements include:

- Those persons or that class of persons who can, from the terms of the trust deed or similar instrument, be identified as having a reasonable expectation to benefit from the trust or other legal arrangement; and
- Those persons who exercise control over the property of the trust or other legal arrangement, including trustees and equivalent persons.

Verifying identification information

4.109 RFIs must verify the following in relation to each trust or legal arrangement:

- Full name of the trust or other legal arrangement;
- Date and place of establishment;
- Legal form, nature and purpose (e.g., discretionary, testamentary, bare);
- Control and ownership structures;
- Official identification number (where applicable); and
- Subject to paragraphs 4.117 and 4.118 below, the identity of all trustees and equivalent persons controlling or having power to direct the activities of the trust or other legal arrangement.

4.110 The RFI should verify the existence, ownership and control structure of the trust or other legal arrangement by:

- Obtaining sight of and retaining appropriate record of the trust deed or equivalent instrument;
- Obtaining sight of and retaining appropriate record of any other instruments or resolutions granting authorisation to carry out business or transactions on behalf of the trust or other legal arrangement; and
- Utilising independent electronic databases.

4.111 In addition, and on the basis of an assessment of the ML/TF risks associated with a customer and its business relationship, RFIs must take reasonable measures to verify the identity of:

- Any donors, settlors, grantors or other persons making the arrangement;

- Any persons whose wishes the trustees or equivalent persons may be expected to take into account;
- Any persons purporting to act on behalf of a trustee or equivalent person;
- Any other parties, including protectors and enforcers; and
- All beneficial owners, as defined in paragraph 4.76.

4.112 All verifications of private individuals associated with trusts and similar arrangements should be carried out in line with the guidance addressing verification of identity for customers who are private individuals.

4.113 Where a trustee or equivalent person is a legal person or arrangement, RFIs should verify the legal person or arrangement as would be done for a customer with the same legal form.

4.114 Where the beneficiaries of a trust or other legal arrangement are designated by characteristics of class, such as the children of a settlor, an RFI should obtain information sufficient to satisfy itself that it will be able to identify and verify the beneficiaries at the time of payout or at the time any beneficiary seeks to exercise a vested right.

4.115 RFIs must carry out verification of the identity of a beneficiary prior to or at the time of any payment, whether direct or indirect, to the beneficiary.

4.116 In most cases, the identity of each trustee or equivalent person should be identified and verified.

4.117 In exceptional circumstances, where the number of trustees or equivalent persons exercising control over management of the trust or other legal arrangement is high, RFIs may use a risk-based approach to determine the identities of individuals to be verified. Where ML/TF risks are standard or low, RFIs should verify at least two of the trustees or other persons exercising control over management of the trust. The individuals verified should be those the RFI expects to hold signatory powers for the purpose of operating an account or exchanging instructions. Those trustees or equivalent individuals who are not verified as signatories should be subject to verification as if they were beneficial owners. Where the money laundering or terrorist financing risks are high, or where a legal arrangement may be seeking to avoid the application of certain CDD measures, the RFI may find it necessary to verify all trustees or equivalent persons.

4.118 Where any individual associated with the trust or other legal arrangement is assessed as higher risk, or where a business relationship is assessed as higher risk for any reason, all trustees and equivalent individuals exercising control over management of the trust or other legal arrangement must be verified.

4.119 Where a customer is a foundation or legal arrangement that differs in control or ownership structure from that of a Bermuda trust, an RFI should establish an understanding of the legal requirements within the legal arrangement's home jurisdiction, such that the RFI is satisfied that it is obtaining and verifying information equivalent to that required by this guidance.

4.120 An RFI should require trustees and equivalent persons to notify it of any material change to:

- Persons who are trustees, beneficial owners or other persons exercising control over management of the trust or other legal arrangement;
- Powers or authorities assigned to such persons; and
- Other changes to the control or ownership structures of the trust or other legal arrangement.

4.121 It is the RFI's responsibility to maintain current information concerning the above.

Unincorporated partnerships and businesses

4.122 Partnerships that are legal persons should be identified and verified using the guidance for legal persons. In such cases, for the purposes of verification, RFIs may obtain sight of and retain record of the following documents in lieu of or in addition to a certificate of incorporation, articles of association or equivalent constitutional documentation:

- Partnership agreement; and/or
- Registered business name certificate.

4.123 Unincorporated businesses, including sole traders and partnerships that are not legal persons, although principally operated by a private individual or group of individuals, differ from private individuals in that there is an underlying business. RFIs should take into account that the underlying business is likely to have a different money laundering or terrorist financing risk profile from that of a private individual.

4.124 Regardless of the features of a particular unincorporated partnership or business, RFIs must use a risk based approach to determine whether the customer and business relationship are legitimate and sufficiently transparent and whether a request for facilities entails any money laundering or terrorist financing risk.

4.125 In addition to the information required for all customers, RFIs must obtain the following identification information in relation to each customer that is an unincorporated partnership or business:

- Full name and any trade names;
- Business address;
- Official identification number (where applicable);

4.126 In line with the guidance for private individuals and legal persons, RFIs must also obtain identification information for the following persons:

- All partners, principals, members, directors and other persons exercising control over the management of the unincorporated partnership or business;
- All persons who, directly or indirectly, ultimately own or control more than 25%, or, in the case of a corporate service provider, 10%, of the customer's property, shares or voting rights; and
- All other persons purporting to act on behalf of the customer or by whom binding obligation may be imposed on the customer.

4.127 RFIs must verify the following in relation to each unincorporated partnership and business:

- Full name;
- Business address;
- Official identification number (where applicable);
- Current existence of the customer;
- Ownership and control structure of the customer;
- Subject to paragraphs 4.132 and 4.133, the identity of all partners, principals, members, directors and other persons exercising control over the management of the unincorporated partnership or business; and
- All other persons purporting to act on behalf of the customer or by whom binding obligation may be imposed on the customer.

4.128 In addition, and on the basis of an assessment of the ML/TF risks associated with a customer and its business relationship, RFIs must take reasonable measures to verify the identity of all persons who, directly or indirectly, own or control more than 25%, or, in the case of a corporate service provider, 10%, of the customer's property, shares or voting rights.

4.129 Where sufficiently independent standard means of verification are not readily available, RFIs should adjust their risk ratings accordingly and consider whether additional precautions are required.

4.130 Where an unincorporated partnership or business is a well-known, reputable organisation with a long history in its industry and with substantial public information concerning it and its principals and controllers, RFIs may consider accepting confirmation of the customer's membership in a relevant professional or trade association as evidence verifying the customer's name and current existence.

4.131 Where an unincorporated partnership or business is less well known or its public profile is lesser or none, RFIs should consider the customer to be a collection of private individuals. In such cases, RFIs should verify the identity of each person named in paragraph 4.126 using the guidance for private individuals.

4.132 In exceptional cases, where the number of partners, principals, members, directors or other persons exercising control over management of the customer is high, RFIs may use a risk-based approach to determine whose identity to verify. Where ML/TF risks are standard or low, RFIs should verify at least two of the relevant signatories and two partners or equivalent persons exercising control over management of the customer. The individuals verified should be those the RFI expects to hold signatory powers for the purpose of operating an account or exchanging instructions.

4.133 Where any individual associated with the customer is assessed as higher risk, or where a business relationship is assessed as higher risk for any reason, all signatories, partners and other individuals exercising control over management of the corporate must be verified.

4.134 An RFI should require customers to notify it of any material changes to:

- Persons who are partners, principals, members, directors, beneficial owners or other persons exercising control over management of the customer;
- Powers or authorities assigned to such persons; and
- Other changes to the control and ownership structures of the customer.

4.135 It is the RFI's responsibility to maintain current information concerning the above.

<u>Employee pension schemes</u>

4.136 Employee pension schemes may take a number of forms. Some may be legal persons or legal arrangements; others may be unincorporated partnerships or businesses.

4.137 Where a customer is:

- an employee benefit scheme or arrangement;

- an employee share option plan;
- a pension scheme or arrangement;
- a superannuation scheme; or
- a similar scheme where contributions are made by an employer or by way of deductions from wages, and the scheme rules do not permit assignment of a member's interest under the scheme,

then RFIs may elect not to identify and verify the employees who are the ultimate beneficiaries of the scheme.

4.138 In such a situation, the principal employer should be identified and verified using the guidance for legal persons and the source of funds should be recorded to ensure that a complete audit trail exists where an employer is wound up.

4.139 In addition, any private individual serving as a scheme administrator, for example, a foundation council member, trustee, scheme manager or other person having control over the business relationship, must be identified and verified using the guidance for private individuals and, where applicable, legal persons.

4.140 In general, the identity of the recipient of any payment of benefits made by or on behalf of a scheme administrator need not be verified. Where, however, individual members of an employment pension scheme are to be given personal investment advice, their identities must be verified. Where the identities of the principal employer and scheme administrators have been satisfactorily verified, and where that verification information is current, RFIs may choose to allow the employer to provide confirmation of the identities of individual employees.

4.141 Where a suspicious transaction trigger event occurs, or where a beneficiary employee, administrator or other person associated with an employee pension scheme poses a higher risk of money laundering or terrorist financing, this exception is not available and enhanced due diligence is required.

Non-profit organisations

4.142 Charities, places of worship, clubs, societies, associations and other non-profit organisations hold their respective titles due to their purposes and may take a number of forms. Some may be legal persons or legal arrangements; others may be unincorporated partnerships, businesses or associations.

4.143 Where an organisation is a legal person, RFIs should, for AML/ATF purposes, treat the organisation in accordance with the guidance for legal persons. The organisation is the RFI's customer, and is, for practical purposes, represented by its directors or equivalent persons who operate the account or otherwise exchange instructions with the RFI.

4.144 Where an organisation is a trust or other legal arrangement, RFIs should, for AML/ATF purposes, treat the organisation in accordance with the guidance for trusts and other legal arrangements. Those trustees or equivalent persons who enter into the business relationship with the RFI in their capacity as trustees of that particular charitable trust or other legal arrangement are the RFI's customers.

4.145 Where any trustee or equivalent person exercising control over the property of a charitable trust or other legal arrangement is not a customer on behalf of the trust or other legal arrangement, RFIs should treat that trustee or equivalent person as a beneficial owner.

4.146 In exceptional cases involving trusts and other legal arrangements, RFIs will need to treat as beneficial owners other private individuals who exercise control, such as receivers appointed to manage the affairs of a charity or place of worship, or settlors or equivalent persons who retain significant power over the property of a trust or other legal arrangement.

4.147 Where an organisation is an unincorporated partnership, business or association, its officers or the members of its governing body are the RFI's customers, who, for AML/ATF purposes, the RFI should treat in accordance with the guidance on private individuals.

4.148 In addition to the information required for all customers sharing the legal form of the organisation, RFIs must obtain the following identification information in relation to each customer that is a non-profit organisation:

- Full name and address;
- Nature of the organisation's activities and objectives;
- Geographic area(s) of operation;
- Identification information for all trustees, directors or equivalent persons; and
- Identification information for all beneficiaries or classes of beneficiaries.

4.149 RFIs may not verify the identity of an unregistered charity, place of worship, club, society, association or other non-profit organisation by referring to a register maintained by an independent, non-government body. Where, however, an organisation has registered with a government body, verification of its existence may be sought by searching an appropriate government registry.

4.150 Registered Bermuda charities are required to file with the Registrar General annual reports that are available for public inspection. RFIs should be aware that although registration indicates that the charity is subject to a level of on-going regulation, registration is not in itself a guarantee of the bona fides of an organisation.

4.151 For the vast majority of non-profit organisations, there will be no private individuals, apart from trustees and equivalent persons, who are beneficial owners within the meaning of the Regulations. RFIs must therefore identify a class of persons who stand to benefit from the activities and objectives of the organisation. This class of persons will often be evident from a review of one or more of the following:

- The charter or constitution of the organisation;
- An extract from a relevant government registry.

4.152 For some organisations, no private individual or class of individuals is named as a direct beneficiary. Examples include charities or clubs for the benefit of animals or flora, or for the conservation or preservation of habitats, the environment or historical buildings.

4.153 Where an independent school or college is a registered charity, RFIs should identify and verify it using the guidance for non-profit organisations. Where such an organisation is not registered as a charity, RFIs should identity and verify it using the guidance for legal persons.

4.154 Non-profit organisations have been known to be used to divert funds to terrorist financing and other criminal activities. RFIs should seek at all times to ascertain whether any customer that is a charity, place of worship, club, society, association or other non-profit organisation is being misused, either:

- By terrorist organisations posing as legitimate entities;
- To exploit legitimate entities as conduits for terrorist financing, including for the purpose of evading asset-freezing measures; or
- To conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

4.155 In assessing the risks posed by different non-profit organisations, RFIs should consider distinguishing between those organisations with a limited geographical remit and those with unlimited geographical scope, such as medical and emergency relief charities, and between those organisations with a limited and local social purpose and those with more sophisticated activities or financial links with other jurisdictions.

4.156 Where an organisation's activity falls outside of the expected scope of the business relationship, or where an RFI's risk rating for the customer is heightened for any other reason, RFIs should consider the extent to which additional evidence is required to dispel any doubts concerning the ML/TF risks associated with the customer and its business relationship with the RFI.

Other entities subject to the Regulations

4.157 Customers that are subject to the Regulations or their equivalent, but that are not regulated in Bermuda or in a jurisdiction that imposes equivalent AML/ATF requirements as an RFI, should be treated according to their legal form. Where such customers are legal persons, RFIs should treat them for AML/ATF purposes in accordance with the guidance for legal persons. Where a customer is an unincorporated partnership or business, RFIs should treat the customer for AML/ATF persons in accordance with the guidance for unincorporated partnerships and businesses. Where a customer is a professional individual acting as, for example a trustee or equivalent person, the professional individual should be identified and verified as for any other private individual.

4.158 Where a customer is an independent professional holding client money in a pooled account, RFIs should have regard to the guidance concerning reliance on third parties.

CHAPTER 5 - NON-STANDARD CUSTOMER DUE DILIGENCE MEASURES

Simplified due diligence

5.1 As a general rule concerning any business relationship or occasional transaction, RFIs must apply the full range of CDD measures, including the requirements to identify and verify the identity of the customer, beneficial owners and any other persons with an ownership interest or controlling interest.

5.2 In limited circumstances, however, where the cumulative ML/TF risks are low, RFIs may consider:

- Applying reduced or simplified CDD measures in accordance with this guidance; or
- Relying upon another person or RFI for the purposes of applying CDD measures.

5.3 The application of simplified due diligence measures is permissible only after assessing the ML/TF risks associated with a business relationship or occasional transaction and the products, services, delivery channels, or geographic location of persons with which the customer engages. Determinations concerning the application of simplified due diligence measures should be made on the basis of any national risk assessment and the risk assessments carried out by the RFI.

5.4 RFIs may consider applying reduced or simplified due diligence measures only where the risk assessment process results in a finding of lower than standard risk.

5.5 RFIs should keep risk findings up-to-date, such that any circumstances affecting the assessed risks are identified and fully considered in determining whether the risk findings remain appropriate or whether they must be revised.

5.6 At all times, the CDD measures applied to any business relationship or occasional transaction should be commensurate with the assessed ML/TF risks.

5.7 Irrespective of whether an RFI ultimately determines that reduced or simplified due diligence is appropriate, the RFI should document its deliberations and the full rationale behind its decision. An RFI should ensure that its documented deliberations and reasoning are available upon request to authorised authorities in order to demonstrate that it has met its CDD requirements.

5.8 Customers for which it may be appropriate to reduce or simplify the application of CDD measures include:

- AML/ATF regulated financial institutions transacting solely on their own behalf (see paragraph 5.146);
- Private individuals for whom receipt of funds may serve as evidence of identity (see paragraphs 4.49 through 4.52);
- Private individuals for whom reduced or alternative documentation may be acceptable for the purposes of identification and verification (see paragraphs 4.53 through 4.60);
- Companies listed on an appointed stock exchange (see paragraphs 4.95 through 4.96);
- Employee pension schemes (see paragraphs 4.136 through 4.141); and
- Bermuda public authorities.

5.9 RFIs contemplating reliance on a third party for the purposes of applying CDD measures should have regard to paragraphs 5.118 through 5.148 of the Guidance Notes.

5.10 In addition, and subject to the above-mentioned risk requirements, reduced or simplified CDD measures may be applicable for certain life insurance products, pension funds, and other low-risk products, provided the following criteria are met:

- The product has a written contractual base;
- Any related transactions are carried out through an account of the customer with an RFI subject to the Regulations, or with an institution that is situated in a country or territory other than Bermuda that imposes requirements equivalent to those in Bermuda, that effectively implements those requirements, and that is supervised for effective compliance with those requirements;
- The product or related transaction is not anonymous and its nature is such that it allows for the timely application of CDD measures where there is a suspicion of money laundering or terrorist financing;
- The product is within the following maximum threshold:
  a) In the case of insurance policies or savings products of a similar nature, the annual premium is no more than $1,000, or there is a single premium of no more than $2,500;
  b) In the case of products that are related to the financing of physical assets where the legal and beneficial title of the assets is not transferred to the customer until the termination of the contractual relationship (whether the transaction is carried out in a single operation or in several operations which appear to be linked) the annual payments do not exceed $15,000;
  c) In all other cases, the maximum threshold is $15,000 per year.

- The benefits of the product or related transaction cannot be realised for the benefit of third parties, except in the case of death, disablement, survival to a predetermined

advanced age, or similar events; and

- In the case of products or related transactions allowing for the investment of funds in financial assets or claims, including insurance or other kinds of contingent claims:
  a) The benefits of the product or related transaction are only realisable in the long term;
  b) The product or related transaction cannot be used as collateral; and
  c) The contract does not permit accelerated payments, early surrender, or early termination.

5.11 RFIs should determine whether particular products meet the criteria for simplified due diligence, and ensure that any reduced or simplified CDD measures applied are commensurate with the assessed risks.

5.12 Where an RFI decides to apply reduced or simplified CDD measures, it must:

- Maintain up-to-date risk findings concerning the products, services, customers, and geographic locations associated with the business;
- Ensure that the level of CDD applied is commensurate with the assessed risks;
- Conduct on-going monitoring of the business relationship;
- Report any knowledge or suspicion of money laundering or terrorist financing; and
- Where relying upon another person or RFI for the purposes of applying CDD, periodically test the quality of the CDD measures the relied upon entity applies and the willingness and ability of the relied upon entity to provide CDD information upon request.

5.13 Where an RFI assesses the risks associated with any business relationship or occasional transaction as anything other than lower than standard, the RFI must discontinue the application of any reduced or simplified CDD measures and apply either standard or enhanced due diligence measures.

5.14 Where there is knowledge or suspicion of money laundering or terrorist financing, or where an RFI has reason to suspect that a customer is acting to avoid the application of standard CDD measures, the RFI must consider whether any reporting requirements have been implicated.

Enhanced due diligence

5.15 Enhanced due diligence is the application of additional CDD measures where necessary to ensure that the measures in place are commensurate with higher ML/TF risks.

5.16 The application of CDD measures commensurate with the ML/TF risks identified allows RFIs to meet two broad objectives. The first is to inform the RFI's periodic and on-going risk assessment processes. The second is to provide a tailored basis for monitoring customer activity and transactions such that attempts to launder money and finance terrorism are more likely to be detected.

5.17 Enhanced due diligence must be applied in all circumstances where the money laundering or terrorist financing risks associated with a customer or the products, services, delivery channels, or geographic location of counterparties with which the customer engages are assessed as higher than standard.

5.18 In addition, enhanced due diligence must be applied in each of the following circumstances:

- The customer has not been physically present for identification purposes (see paragraph 5.26 through 5.30);
- The business involves a correspondent banking relationship (see paragraph 5.148);
- The business relationship or occasional transaction involves a politically exposed person (see paragraphs 5.97 through 5.117);
- The business relationship or occasional transaction has a connection with a country or territory that represents a higher risk of money laundering, corruption, terrorist financing or being subject to international sanctions.

5.19 A business relationship or occasional transaction has a connection with a country or territory that represents a higher risk of money laundering, corruption, terrorist financing or being subject to international sanctions where a relevant person is:

- The government or a public authority within the country or territory;
- A politically exposed person in relation to the country or territory;
- A person who is a resident in, citizen of, or incorporated in the country or territory;
- A person having a registered office or other business address in the country or territory;
- A person whose funds are or derive from either income arising in the country or territory, or assets held in the country or territory by or on behalf of the person;
- Transacting from or with the country or territory.

5.20 For the purposes of paragraph 5.19, a relevant person is any of the following:

- A customer;
- A beneficial owner or controller of the customer;
- A third party for whom the customer is acting;

- A beneficial owner or controller of a third party for whom the customer is acting; or
- A person acting, or purporting to act, on behalf of the customer.

5.21 Where an RFI determines that enhanced due diligence measures are necessary, it must apply specific and adequate measures to compensate for the higher risk of money laundering.

5.22 In selecting the appropriate additional measures to be applied, RFIs should consider obtaining additional information and approvals, including one or more of the following:

- Additional information on the customer, such as occupation, volume of assets, and information available through public databases;
- Additional information on the nature and purpose of the business relationship (see paragraphs 4.1 through 4.4);
- Additional information on the source of funds and source of wealth of the customer (see paragraphs 5.110 through 5.113);
- Additional information on the reasons for planned or completed transactions; and
- Approval of senior management to commence or continue the business relationship (see paragraph 5.109).

5.23 In addition, RFIs should consider applying additional measures, such as:

- Updating more frequently the identification and verification data for the customer, its beneficial owner(s), and any other persons with an ownership or controlling interest;
- Conducting enhanced monitoring of the business relationship by increasing the number and frequency of controls applied and by identifying patterns of transactions requiring further examination; and
- Requiring the first payment to be carried out through an account in the customer's name via an RFI subject to the Regulations, or via an institution that is situated in a country or territory other than Bermuda that imposes requirements equivalent to those in Bermuda, that effectively implements those requirements, and that is supervised for effective compliance with those requirements;

5.24 Where an RFI knows of or suspects money laundering or terrorist financing or where an RFI has doubts as to the veracity or adequacy of documents, data, or information obtained for the purposes of identification or verification, enhanced CDD is required. In these circumstances, there is no discretion as to whether or not to apply enhanced CDD.

5.25 Irrespective of whether an RFI ultimately determines that enhanced due diligence is appropriate, the RFI should document its deliberations and the full rationale behind its

decision. An RFI should ensure that its documented deliberations and reasoning are available upon request to authorised authorities.

Non face-to-face identification and verification

5.26 The volume and types of non-face-to-face transactions have increased with the use of communications via post, telephone and internet. RFIs must take specific and adequate measures to assess the risks associated with such transactions and to compensate for any higher risks.

5.27 In limited circumstances, and only where the risk of money laundering or terrorism financing is assessed as low, limited exceptions (see paragraphs 3.13 through 3.16) may be available.

5.28 In most circumstances, RFIs must take additional measures commensurate with the risks identified. Such measures may include:

- Ensuring that the customer's identity is established by additional documents, data or information;
- Further verification or certification of the documents acquired, for example by obtaining confirmatory certification by an RFI subject to the Regulations, or by an institution that is situated in a country or territory other than Bermuda that imposes requirements equivalent to those in Bermuda, that effectively implements those requirements, and that is supervised for effective compliance with those requirements; and
- Requiring the first payment to be carried out through an account in the customer's name via an RFI subject to the Regulations, or via an institution that is situated in a country or territory other than Bermuda that imposes requirements equivalent to those in Bermuda, that effectively implements those requirements, and that is supervised for effective compliance with those requirements.

5.29 RFIs should be cognizant of the risks associated with customers approaching an RFI by post, telephone or internet in a deliberate effort to avoid face-to-face contact.

5.30 RFIs should at all times be cognizant of the inherent risk of impersonation fraud associated with non-face-to-face identification and verification and should have regard to paragraph 4.42.

Enhanced due diligence for wire transfers

5.31 **Chapter 8 - Wire Transfers** sets forth general guidance for RFIs that are payment service providers (PSPs) carrying out transfers of funds as payer PSPs, intermediary PSPs and payee PSPs.

5.32 Regulation 11 requires each RFI that is a PSP to apply appropriate enhanced due diligence measures to transfers of funds presenting higher risks of ML/TF, including transfers involving:

- A higher-risk person or jurisdiction;
- International sanctions;
- A customer who has not been physically present for identification purposes;
- A non-Bermuda correspondent bank;
- A politically exposed person (PEP); or
- Any other situation, which, by its nature can present a higher risk of money laundering or terrorist financing.

5.33 Additional factors may cause a PSP to conduct enhanced due diligence on a transaction prior to authorizing the transfer. These factors include, but are not limited to:

- The PSP's risk tolerance and risk assessments;
- The involvement of any third party service provider;
- The particular nature of the transfer that has been requested, in the context of the accountholder's previous transactions and conduct.

5.34 PSPs should consider all aspects of sending, forwarding and receiving a transfer of funds as factors in assessing whether enhanced due diligence is required, and whether the transfer of funds, or any related transaction, is suspicious. Circumstances that may indicate a transfer of funds, or any related transaction, is suspicious, and to which enhanced due diligence measures should be applied, include, but are not limited to:

- A payer who is unwilling or unable to provide the required complete information;
- A payer for whom the complete information cannot be verified, where it is required to do so;
- A payer seeking to alter the customer information sent via the messaging system, for reasons that the PSP is not able to fully confirm as legitimate;
- A payer seeking to route the transaction through apparently unnecessary intermediary PSPs;
- A payer seeking to ensure that the complete information does not reach all PSPs involved in the execution of the payment;

- A transfer with missing, meaningless or otherwise incomplete information;
- A transfer of funds in an amount greater than $1,000 to a non-account holder, particularly where no unique identifier accompanies the transfer;
- A transfer for which a PSP knows or suspects that information provided by the payer PSP has been stripped or altered at any point in the payment chain;
- A transfer for which there is evidence to suggest that a person other than the named payee is the intended final recipient.

5.35 Where a PSP becomes aware in the course of processing a payment that it is missing required information, or that the required information provided is meaningless or otherwise incomplete, the payee PSP must:

- Reject the transfer;
- Request the complete information on the payer and payee; or
- Make an internal suspicious activity report to the Reporting Officer.

5.36 Where a payer PSP or intermediary PSP regularly fails to provide all required information on the payer and payee, the payee PSP should have regard to paragraphs 8.56 through 8.58.

New payment methods

5.37 New payment methods (NPMs) are recent and on-going technological innovations in payment and value transfer systems, including, but not limited to:

- Pre-paid cards and tokens;
- Payments by mobile phone;
- Internet-based payment systems; and
- Payments involving virtual currencies.

5.38 RFIs must meet their AML/ATF obligations under the Acts and Regulations and must determine appropriate policies, procedures and controls for all of their business, including any NPMs.

5.39 This portion of the guidance provides additional information about challenges that NPMs present, and additional appropriate measures for conducting enhanced due diligence and mitigating risk, as a supplement to those measures described elsewhere in these guidance notes. Many of the following paragraphs are appropriate for most or all NPMs. Where noted, guidance is also provided in relation to specific categories of NPMs.

5.40 RFIs must assess the risks associated with NPMs and apply appropriate enhanced due diligence and ML/TF risk mitigation measures.

5.41 An initial risk assessment should be conducted prior to offering an NPM or entering into a business relationship with an NPM product or service provider. The risks associated with each NPM or NPM product or service provider should also be assessed on an on-going basis.

5.42 When assessing the risks associated with offering an NPM or entering into a business relationship with an NPM product or service provider, RFIs should ensure that they assess the risks associated with each of the particular persons involved with an NPM, and not only the risks associated with an NPM product or service itself. For additional information, see paragraphs 5.83 through 5.96.

5.43 Many NPMs, or the services associated with NPMs do not fall neatly into the categories described in paragraph 5.37 or they offer functionality involving more than one of those categories. Despite the range of NPMs in existence, several challenges are common to many NPMs. These challenges include the non-face-to-face nature of many NPM transactions, the possibility of anonymity that some NPMs offer, and the difficulty of monitoring person-to-person payments that may cross international borders and involve a range of regulated or unregulated service providers.

5.44 Each RFI should be aware of the differences in the risks posed by an NPM that the RFI itself offers, as compared with the risks posed by an NPM product or service provider that enters into a business relationship with an RFI. Each RFI should tailor its enhanced due diligence measures accordingly.

5.45 NPMs can develop and evolve rapidly. RFIs that contemplate offering NPMs or entering into business relationships with NPM product or service providers should stay abreast of industry best practices and both national and international standards involving NPMs and the risks associated with them.

NPM risk factors and risk mitigation measures

5.46 RFIs should have policies, procedures and controls in place to prevent the misuse of NPMs for the purposes of ML/TF.

5.47 An RFI's policies, procedures and controls should be commensurate with the risks it faces. For additional information, see **Chapter 2: Risk-Based Approach**.

5.48 Each individual NPM and each NPM product and service provider has a unique set of features and persons associated with it. In assessing the features and persons associated with an individual NPM or NPM provider, RFIs should be aware of risk factors that are common to many NPMs. These risk factors include, but are not limited to:

- A lack of face-to-face interaction between the RFI, the customer and any third parties;
- Any possibility to transact anonymously;
- No limits, or high limits, on transactions;
- Cross-border transactions;
- Person-to-person transactions;
- Restrictions that preclude the transfer of information needed for effective CDD;
- An inability to monitor transactions within an NPM's system; and
- The use of service providers or agents that are not subject to effective AML/ATF regulation.

5.49 Where an RFI identifies higher risks in connection with offering an NPM or entering a business relationship with an NPM product or service provider, it must take reasonable and appropriate steps to mitigate and manage those higher risks. Reasonable and appropriate steps may be called risk mitigation measures, or enhanced due diligence measures. In practice, there may be no distinction between the two.

5.50 NPM risk-mitigation measures may be considered as falling within several broad categories:

- CDD;
- Usage limits;
- Geographic limits;
- Monitoring and record-keeping; and
- Segmentation due diligence and controls.

NPM customer due diligence

5.51 RFIs should mitigate the risks associated with a lack of face-to-face interactions and the potential for anonymity by applying an appropriate, risk-based approach to CDD for NPMs.

5.52 For general guidance on non-face-to-face identification and verification, see paragraphs 5.26 through 5.30.

5.53 Where an RFI enters into a relationship with an NPM product or service provider, it should ensure that it understands and approves of the AML/ATF policies, procedures and controls

the NPM provider has in place. For additional information, see paragraphs 5.83 through 5.96.

5.54 Nothing in the Acts or Regulations permits RFIs to engage in anonymous transactions. Where an RFI is unable to apply CDD measures in accordance with the Regulations, Regulation 9 requires the refusal or termination of the business relationship or transaction.

5.55 Where an NPM provides for anonymous transactions in very small amounts, and only on an infrequent basis, the risks associated with anonymity may appear to be lower. In reality, however, an absence of CDD impedes an RFI's ability to effectively monitor an NPM to ensure that transactions are not linked, and that they remain small and infrequent. An absence of CDD also increases the likelihood of impersonation and other types of fraud that may be costly and damaging to an RFI and its customers.

5.56 When an NPM offers any potentially anonymous functionality, whether when a customer purchases or enters into a business relationship with the NPM, when registering or when adding, spending, transferring or withdrawing value, an RFI should engage with the NPM only after taking appropriate measures to mitigate the associated risks.

5.57 Where an NPM features limited CDD on low value and infrequent transactions, an RFI should require customer identification and verification for transactions above an appropriate risk-based threshold amount and/or frequency.

5.58 Where an NPM account may be used to effect a transfer of value from one person to another, RFIs should have regard to the guidance provided in **Chapter 8: Wire Transfers**, and in particular to paragraphs 8.66 through 8.67. As required, RFIs should obtain and, where appropriate, verify the identity of any recipient of funds.

5.59 When an NPM offers any potentially anonymous functionality, RFIs should aggregate NPM account information by collecting, retaining and analysing all relevant information that accompanies a transaction through the NPM. The aggregation of customer and transaction information can enable the RFI to more effectively identify activity that is linked and, collectively, exceeds any threshold amount or frequency, or appears abnormal or suspicious.

5.60 In order to aggregate customer and transaction information, RFIs should identify transactions and accounts that are linked to the same IP address, e-mail address, telephone number, common funding source, or more traditional CDD information such as a customer's name, physical address, date of birth, or identity number.

5.61 Where an NPM allows a user to anonymously register for or otherwise access an NPM, RFIs should seek to ensure that transfers of value into the NPM, or withdrawals of value from the NPM, are possible only using an account, such as a bank or credit card account, that has been subjected to the identification and verification processes of an RFI subject to AML/ATF regulation in Bermuda or in another jurisdiction that imposes equivalent AML/ATF standards.

5.62 RFIs should be aware of the possibility of person-to-person payments within an NPM system, which may allow an NPM account to send or receive significant value from other NPM accounts without ever interacting with a verified bank or credit card account. In such cases, RFI's should monitor transactions between the NPM account and the RFI for any abnormal or suspicious activity.

5.63 Where an RFI's customer is an NPM provider, and the NPM provider has access to customer information the RFI does not, the RFI should seek to apply the guidance provided in paragraphs 5.83 through 5.96.

NPM Usage limits

5.64 RFIs should mitigate the risks associated with a lack of face-to-face interactions and the potential for anonymity by implementing appropriate usage limits for NPMs.

5.65 Usage limits are restrictions on the value, frequency and types of transactions that an NPM can facilitate. The higher the ML/TF risks associated with an NPM are, the stronger and more numerous the usage limits should be. A lack of usage limits, or overly generous usage limits, should generally be considered higher risk for ML/TF.

5.66 Examples of usage limits include restrictions on:

- The amount of value that can be loaded into, transacted within or spent or withdrawn from an NPM in a given period of time;
- Funding sources, including restrictions on the acceptance of cash;
- The withdrawal of cash from an NPM via ATM or other method;
- The number or types of third parties able to send or receive value using an NPM; and
- The number of accounts a person may hold with an NPM.

5.67 Where an NPM has a reduced CDD requirement, RFIs should consider limiting the NPM to a single, low-value, non-reloadable use.

5.68 RFIs may consider limiting the utility of an NPM solely to person-to-business transactions.

5.69 Where person-to-person transactions are possible, RFIs should use a risk-based approach to limit the value or frequency of those transactions. In considering the risks associated with person-to-person transactions, an RFI should consider whether it has access to sufficient CDD and transaction information on all parties to the transactions and the ability to effectively monitor transactions in an on-going manner.

5.70 RFIs may also consider requiring payments into or from the NPM system to be carried out via an account that has been subjected to the identification and verification processes of an AML/ATF-regulated RFI. See paragraph 5.61.

5.71 RFIs should ensure that an NPM account may be frozen or blocked when deemed necessary.

NPM Geographic limits

5.72 RFIs should consider whether any geographic limits, including any limits on cross-border functionality, must be placed on an NPM in order to mitigate the ML/TF risks associated with the NPM.

5.73 RFIs should consider the geographic scope of expected use of a particular NPM, and determine whether the use of an NPM outside of that geographic scope would be suspicious.

5.74 RFIs should ensure that appropriate geographic limits are put in place where:

- There is insufficient justification for an NPM to be used outside of a particular geographic area;
- The risks presented exceed an RFI's risk tolerance; or
- A particular geographic area is subject to international sanctions.

5.75 Where an RFI enters into a business relationship with an NPM product or service provider, the RFI should consider whether the NPM provider is operating from or in any jurisdiction that poses a higher risk of ML/TF, from or in any geographic area subject to international sanctions, or any jurisdiction where the NPM provider is not subject to adequate AML/ATF regulation and oversight.

5.76 RFIs should use IP addresses as one indicator of the geographic location of an NPM customer or service provider, bearing in mind that proxy servers and other protocols may mask a user's true location, and bearing in mind that an NPM provider's IP address may not be indicative of the jurisdiction in which the NPM provider is regulated.

NPM Monitoring and record-keeping

5.77 RFIs should ensure that they are able to effectively monitor NPM transactions for any unusual or suspicious activity, and for compliance with international sanctions.

5.78 As with any financial product or service, RFIs should establish norms for NPM transactions and conduct and identify any activity that fall outside of those norms. For additional information on establishing norms, see paragraphs 7.11 through 7.14.

5.79 RFIs should use on-going monitoring to determine an appropriate level of CDD, usage limits and geographic limits. Where monitoring indicates a significant change in the way an NPM is used, for example, a customer attempting to use an NPM to carry out a transaction that is larger than the customer's verified identity information will permit, RFIs should apply any required CDD or implement any appropriate usage or geographic limits prior to determining whether to allow the transaction to proceed.

5.80 Where an RFI itself offers an NPM, it will have access to all customer and transaction information and should conduct appropriate risk-based monitoring.

5.81 Where an RFI establishes a business relationship with an NPM product or service provider, it may not have direct access to all customer and transaction information. In such cases, RFIs should apply the guidance provided in paragraphs 5.83 through 5.96.

5.82 RFIs should maintain records of all relevant NPM customer and transaction information, including IP and e-mail addresses, in accordance with the guidance provided in **Chapter 11: Record-Keeping**.

NPM Segmentation due diligence and controls

5.83 RFIs should put in place appropriate policies, procedures and controls to mitigate the risks associated with the segmentation of an NPM product or service between different persons and jurisdictions.

5.84 RFIs should ensure that they understand all of the parties involved with an NPM, and the risks associated with each. Some NPMs may be managed entirely by the issuing entity. However an NPM may also involve an issuing entity, a branded transaction service provider, and a range of exchangers, distributors, agents and other persons involved in sales, loading value, transferring value, spending value and withdrawing value. All types and combinations of NPMs, including pre-paid cards, mobile payments, internet payment systems and payments involving virtual currency may involve a broad range of persons.

5.85 Risks associated with the segmentation of an NPM product or service between different persons and jurisdictions include, but are not limited to:

- Difficulty in conducting effective CDD;
- Difficulty in conducting on-going monitoring;
- Loss of information, or an inability to access information;
- Unclear lines of communication and accountability; and
- The involvement of NPM providers not subject to appropriate registration, licensing and AML/ATF regulation requirements.

5.86 Both prior to entering into a business relationship with an NPM product or service provider, and throughout any such relationship, an RFI should assess whether and how each person and jurisdiction involved in the NPM may affect the RFI's ability to fulfil its obligations under the Regulations and these Guidance Notes. Where all risks identified and assessed can be effectively and appropriately mitigated, those risks should be mitigated. Where all risks identified and assessed cannot be effectively mitigated, an RFI should not enter into the business relationship.

5.87 RFIs considering a business relationship with an NPM provider should carry out due diligence as to the NPM provider under consideration. The purpose of the due diligence is to determine whether the NPM provider has the ability, capacity, and any required authorisation to implement appropriate AML/ATF policies, procedures and controls. RFIs should establish a written policy concerning the scope and frequency of initial and on-going due diligence carried out as to such NPM providers.

5.88 At a minimum, RFIs carrying out due diligence as to an NPM service provider should consider the following:

- Whether the NPM service provider is licensed or otherwise authorised to carry out the NPM's activities;
- Whether, where relevant, the service provider is effectively regulated;
- Whether the scope of any regulation includes compliance with the AML/ATF regulations of Bermuda or of a jurisdiction that imposes equivalent AML/ATF requirements;
- Whether any operational, financial, human resource, structural, legal, or regulatory considerations may affect the service provider's ability to carry out effective CDD and on-going monitoring, where relevant, or impede the RFI's access to relevant information held by the NPM service provider, including customer and transaction information;

- Whether any confidentiality, secrecy, privacy, or data protection restrictions may impede the RFI or any relevant Bermuda regulatory authorities from effectively monitoring the activities of the NPM service provider.

5.89 Where an RFI is considering a business relationship with an NPM provider that is not subject to AML/ATF regulation in Bermuda, or that is not in a jurisdiction that imposes equivalent standards, the RFI should ensure that the NPM provider has appropriate CDD policies, procedures and controls in place. Telecommunications companies, for example, that provide NPM payment intermediary services often hold customer information, but due diligence is required to determine whether that customer information has been obtained and maintained in accordance with the appropriate AML/ATF standards.

5.90 RFIs must not enter into business relationship with an NPM provider where access to required data without delay is likely to be impeded by confidentiality, secrecy, privacy, or data protection restrictions.

5.91 Where an RFI is establishing a business relationship with an NPM provider that is not subject to appropriate AML/ATF regulation, and where the RFI does not have ready access to appropriate transaction and customer information of an NPM product or service provider, the customer agreement between the RFI and NPM provider should confirm that an RFI will receive, upon request, transaction and customer information on users of the NPM.

5.92 The customer agreement should authorise the RFI to continuously monitor and assess the NPM provider against the terms of the agreement in order to ensure that any necessary corrective measures are taken promptly. The level of monitoring and assessment authorised by the customer agreement should be proportionate to the risks involved with the NPM's activities.

5.93 The customer agreement should permit the RFI to periodically test whether the NPM provider complies with requests for information, and should entitle the RFI to terminate the relationship where the NPM service provider fails to perform according to the agreement.

5.94 The customer agreement should clarify the respective roles of the RFI and the NPM provider as regards compliance with international sanctions. For additional information, see paragraphs 6.66 through 6.69.

Agent networks and other third parties

5.95 Where an NPM or other money value transfer business involves an agent network, or other third parties, RFIs should ensure that the product or service provider has in place appropriate

policies, procedures and controls to assess and mitigate the risks associated with the involvement of agents and third parties. RFIs should require product and service providers to demonstrate that they have conducted appropriate background and reference checks on any agents or third parties.

5.96 RFIs should also require product and service providers to demonstrate that that its agents or third parties are examined for compliance with appropriate AML/ATF obligations and that appropriate policies, procedures and controls provide for on-going training and supervision of the agents or third parties.

Politically exposed persons (PEPs)

5.97 Individuals who have or have had a high political profile, or hold or have held public office, can pose a higher risk to RFIs as their position may be abused for money laundering and related predicate offences such as corruption and bribery, as well as for the financing of terrorism and proliferation. This risk also extends to members of their families and to close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the customer, beneficial owner, or other person with an ownership or controlling interest into a higher-risk category.

Definitions of PEPs: including foreign, domestic and international organisation PEPs

5.98 A PEP is defined in Regulation 11 as an individual who is or has been entrusted with a prominent public function by a foreign country or territory outside Bermuda (Foreign PEP), by an international organisation (International Organisation PEP), or in Bermuda (Domestic PEP). The application of anti-money laundering and anti-terrorism financing regulations concerning PEPs also extends to members of their immediate families and to close associates.

5.99 The application of AML/AFT regulations concerning PEPs extends to the following persons:

<u>Foreign and domestic PEPs:</u>

- Heads of state, heads of government, ministers and deputy or assistant ministers;
- Members of parliament and senior political party officials;
- Senior government officials including Permanent Secretaries;
- Members of supreme courts, constitutional courts, or other high level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances;
- Members of the boards of central banks;

- Ambassadors and charges d'affaires;
- High-ranking officers in the armed forces; and
- Members of the administration, management or supervisory bodies of state-owned enterprises.

International organisation[1] PEPs include:

- Senior management;
- Directors and deputy directors; and
- Members of the board.

The above categories are not exhaustive but do not include middle-ranking or more junior officials. Public functions exercised at levels lower than national should normally not be considered prominent.

However, when their political exposure is comparable to that of similar positions at national level, RFIs should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs.

Family members of PEPs:

- A spouse;
- A partner (including a person who is considered by national law as equivalent to a spouse);
- Children and their spouses or partners;
- Parents; and
- Siblings.

Close associates of PEPs:

- Partners outside the family unit such as girlfriends, boyfriends, and mistresses;
- Prominent members of the same political party, civil organisation, labour or employee union;
- Individuals who have joint beneficial ownership of a legal entity or legal arrangement with a PEP;
- Individuals who have sole ownership of a legal entity or legal arrangement that have been set up for the benefit of a PEP; and

[1] International Organisation has its meaning found in Regulation 2 of the Proceeds of Crime Act (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008

- Individuals with any other close business relations with a PEP, including through joint membership of a company board.

Determination of PEP status

5.100 RFIs must utilise risk-based procedures to determine whether the customer or beneficial owner is a foreign PEP, domestic PEP, or international organisation PEP.

On-going monitoring

5.101 RFIs are required to conduct on-going monitoring to identify whether existing customers, beneficial owners, and other persons with ownership or controlling interests have become PEPs after the initial establishment of the business relationship. Such on-going monitoring should cover both the business relationship and public information relating to possible changes in the status of its customers with regard to political exposure. Guidance on the on-going monitoring of the business relationship is provided in paragraphs 8.1 through 8.17.

Life insurance policies

5.102 Life insurance providers must have risk-based procedures to determine whether the beneficiaries of a life insurance policy and/or the beneficial owners of the beneficiary are foreign or domestic PEPs. In cases where the life insurance company did not have a customer relationship with the beneficiaries, the company should conduct CDD and determine any PEP status when preparing for the pay-out.

Time limit

5.103 RFIs should apply a risk-based approach in determining whether an individual who has been entrusted with a prominent public function but no longer holds that position should still be handled as a PEP. At a minimum, such an individual should be handled as a PEP for a period of one year after leaving office. Possible risk factors for handling an individual as a PEP for an extended period of time include:

- The level of (informal) influence that the individual could still exercise;
- The seniority of the position that the individual held as a PEP; and
- The linkage (both formal and informal) between the individual's previous and current positions and functions.

5.104 For the purpose of deciding whether an individual is a PEP or a family member or close associate of a PEP, RFIs should rely first and foremost on the information obtained through the application of CDD measures. Where RFIs need to carry out additional checks and verify information, they may rely upon a wide range of sources including internet and media searches, social media, and commercial databases.

Commercial PEPs databases

5.105 RFIs may use a subscription to a specialist PEP database as part of their overall effort to identify PEPs and mitigate their risk. However, RFIs should take into account the limited nature of PEPs databases and should use them only as additional sources of information on higher-risk individuals and not as the primary or sole risk-mitigation tool. RFIs should not assume that a customer is not a PEP or a family member or close associate of a PEP solely due to the lack of a name in a PEPs database.

Risk-based enhanced due diligence

Foreign PEPs

5.106 RFIs should consider all foreign PEPs to be high-risk and require enhanced due diligence. With regards to foreign PEPs, in addition to performing normal CDD, RFIs must:

- Obtain appropriate senior management approval for establishing a business relationship with such a customer and for continuing a business relationship with an existing customer who has become a PEP;
- Take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or occasional transaction; and
- Conduct enhanced on-going monitoring of the business relationship.

Domestic and international organisation PEPs

5.107 RFIs should have procedures in place to assess the risk of the business relationship with domestic and international organisation PEPs. Where the business relationship with a domestic or international organisation PEP is not classified as high-risk, the RFI should apply standard CDD measures and monitoring, and can treat the PEP as a standard customer. However, when the business relationship with a domestic or international organisation PEP is classified as high-risk, in addition to performing normal CDD, RFIs must:

- Obtain appropriate senior management approval for establishing a business relationship with such a customer and for continuing a business relationship with an existing customer who has become a PEP;
- Establish the source of wealth and source of funds that are involved in the business relationship or occasional transaction; and
- Conduct enhanced on-going monitoring of the business relationship.

Life insurance and trust beneficiaries who are PEPs

5.108 Life insurance companies and trust businesses should have procedures in place to assess the risk of the business relationship with PEPs, including the pay-out of life insurance policies or the exercise of a vested right in which the beneficiaries or their beneficial owners are PEPs. When the business relationship with a PEP is classified as high-risk, in addition to performing normal CDD, life insurance companies and trust businesses are required to:

- Notify senior management before the pay-out of policy proceeds or the exercise of a vested right; and
- Conduct enhanced scrutiny on the whole business relationship involving the PEP.

Senior management approval and notification

5.109 For the purpose of seeking approval from senior management for establishing or continuing a high risk business relationship, such as with a PEP, or for notifying senior management before the pay-out of a life insurance policy or the exercise of a vested right involving a PEP, senior management has the meaning given in paragraph 1.16 of these guidance notes. Senior management approval does not necessarily mean obtaining approval from the board of directors or equivalent body. The member of senior management who grants or denies approval should have deep knowledge of the RFI's AML/ATF procedures, a strong understanding of the business relationship and/or PEP's ML/TF risk profile, and preferably active involvement in the approval process of the RFI's AML/ATF policies and procedures. In most cases, the Compliance Officer referred to in paragraph 1.36 of these guidance notes should be responsible for receiving notifications and requests for approval.

Source of wealth and source of funds

5.110 For the purposes of establishing the source of wealth of a PEP or other relevant person, the source of wealth means the origin of the person's total assets. The information on the source

of wealth should provide an indication of the person's volume of wealth and a general understanding of how the person acquired that wealth.

5.111 For the purposes of establishing the source of funds that are involved in the business relationship or occasional transaction with a PEP or other relevant person, the source of funds means the origin of the particular funds or other assets that are involved in the business relationship or occasional transaction. The information concerning the source of funds should be substantive and go beyond the financial institution and account from which the funds were transferred to include details such as the identity of the sender (or recipient) and the reason for receiving (or sending) the funds.

5.112 For the purposes of establishing the source of wealth and source of funds of a PEP or other relevant person, RFIs may rely upon declarations by the person. However, an inability of the RFI to verify the person's declaration of the source of wealth or source of funds should be taken into account when establishing the value of the information provided. In addition, discrepancies between the person's declaration and information obtained from other sources or refusal of the person to disclose relevant information on the source of wealth or source of funds may be considered as red flags.

5.113 Where researching and verifying the accuracy of a person's declaration of the source of wealth or source of funds, RFIs may rely upon a wide range of sources to reveal information about the person's wealth, income, specific assets, and lifestyle. Possible sources include databases concerning legal and beneficial ownership such as publicly available property registers, land registers, asset and income disclosure registers, and company registers, as well as past transactions (for existing customers), internet and media searches (for high profile persons) and social media.

<u>Level of risk of the business relationship with domestic and international organisation PEPs</u>

5.114 When determining whether the business relationship with a domestic or international organisation PEP should be classified as high-risk, RFIs should consider risk factors, including whether the PEP:

- Has business interests that are related to his/her public functions;
- Is involved in public procurement processes;
- Is from a country or territory country or territory that represents a higher risk of money laundering, corruption, terrorist financing or being subject to international sanctions;

- Has a prominent public function in industries known to be exposed to high levels of corruption, such as the oil and gas, mining, construction, natural resources, defence, sports, gaming and gambling industries; or
- Has a prominent public function that would allow him/her to exert a negative impact on the effective implementation of the international AML/ATF standards in Bermuda. Such public functions could include the governor, the premier, key ministers and other political or parliamentary leaders.

5.115 Where RFIs need to carry out research to determine the level of risk of the business relationship with a domestic or international organisation PEP, they may rely upon a wide range of sources. Possible sources include internet and media searches as well as relevant reports, evaluations, and databases on AML/ATF and corruption risk published by national, international, and non-governmental organisations, which may provide valuable information and background on the PEP's country or territory and highlight specific issues and industries of concern. Resources such as AML/CFT mutual evaluation reports, which assess the compliance of countries with the international AML/CFT standards (available on the FATF website at: www.fatf-gafi.org) and Transparency International's Corruption Perceptions Index (available at www.transparency.org), which ranks over 170 countries and territories according to their perceived level of corruption, may be helpful in assessing the level of risk.

Enhanced on-going monitoring

5.116 When conducting enhanced on-going monitoring of the business relationship with a PEP, RFIs should have regard to paragraphs 5.15 through 5.25. RFIs should also be aware of the red flags and indicators that can be used to detect a PEP's abuse of the financial system. RFIs should have regard to the FATF list of PEP-specific red flags and indicators for suspicion (available at www.fatf-gafi.org) and other relevant sources to assist in the detection of a PEP's abuse of the financial system.

5.117 Guidance on meeting AML/ATF obligations in cases where a customer is an existing customer of another RFI in the same group is provided in paragraphs 5.140 through 5.142.

Multipartite relationships, including reliance on third parties

Reliance on third parties

5.118 An RFI may choose to rely upon another person or institution (a third party) to apply certain CDD measures, provided that both the third party and the nature of the reliance meet certain criteria. In any reliance situation, however, the relying RFI retains responsibility for any

failure to comply with a requirement of the Regulations, as this responsibility cannot be delegated.

5.119 The CDD measures that an RFI may rely upon a third party to apply are:

- Identifying the customer and verifying the customer's identity;
- Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner;
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

5.120 In any reliance situation, the following duties remain with the relying RFI and cannot be delegated:

- The duty to conduct on-going monitoring to scrutinise transactions undertaken throughout the course of the relationship to ensure that the transactions are consistent with the RFI's knowledge of the customer, beneficial owner, purpose and intended nature of the business relationship and, where necessary, the source of funds or wealth; and
- The duty to report knowledge or suspicion of money laundering or terrorist financing.

5.121 RFIs may rely upon a third party who is:

<u>For Bermuda persons</u>

- An AML/ATF regulated financial institution under Section 2(2) of the Regulations; or
- A specified business under Section 3 of the Anti-Terrorism (Financial and Other Measures) (Business in Regulated Sector) Order 2008; or
- An independent professional as defined at Section (2)(1) of the Regulations; and
- Regulated, supervised or monitored for, and has measures in place for compliance with the AML/ATF Regulations of Bermuda.

<u>For non-Bermuda persons</u>

- An institution that carries on business corresponding to the business of an AML/ATF regulated financial institution or independent professional; and
- Regulated, supervised or monitored for, and has measures in place for compliance with AML/ATF regulations equivalent to those of Bermuda.

<u>Limitations to reliance</u>

5.122 Reliance on a third party to apply certain CDD measures cannot be absolute. For one RFI to rely upon the verifications carried out by a third party, the verification that the third party has carried out must have been based upon at least the standard level of customer verification. With the exception of situations in which an underlying customer is confirmed as falling under Regulations 10(2), 10(3), 10(4) or 10(5), it is not permissible to rely upon simplified due diligence carried out.

5.123 Regulations 10(2), 10(3), and 10(5) apply where the customer is acting on its own behalf, and not for any underlying customer. See paragraphs 5.146 through 5.147.

5.124 Where the customer is an independent professional (or similar professional) and the product is an account into which monies of underlying customers are pooled, Regulation 10(4) permits simplified due diligence on the independent professional (or similar professional) only where the following conditions are met:

- The pooled account is held in Bermuda by an independent professional subject to, and supervised for compliance with, Bermuda's AML/ATF Acts and Regulations; and
- The institution holding the pooled account has confirmed in writing, and confirms, via periodic testing, that it will receive, upon request, information on the identity of the underlying customers whose monies are pooled in the account.

Or

- The pooled account is held by an independent professional (or similar professional) in a country or territory other than Bermuda that imposes equivalent AML/ATF requirements; and
- The independent professional (or similar professional) is supervised for compliance with that jurisdiction's AML/ATF requirements; and
- The institution holding the pooled account has confirmed in writing, and confirms, via periodic testing, that it will receive, upon request, information on the identity of the underlying customers whose monies are pooled in the account.

5.125 RFIs may rely upon another person or institution to carry out CDD measures only when the person or institution being relied upon confirms in writing that the measures have actually been applied. An RFI that has relied upon another person to apply certain CDD measures may not ''pass on'' verification to a third institution.

5.126 For an institution to confirm that it has carried out CDD measures in respect of a customer is a serious matter. A third party must not claim to have verified a customer on the basis of a

generalised assumption that its systems have operated effectively. There must be awareness that the appropriate verification steps have in fact been taken in respect of the customer.

Notification and consent

5.127 RFIs should provide the third party with written notification of the reliance. The notification should specify that the RFI intends to rely upon the third party institution for the purposes of Regulation 14(1)(a). Examples of ways this notification may be delivered are:

- Where one institution introduces a client to another institution, the issue of reliance is raised during the introduction process and is part of the formal agreement with the intermediary.
- Where the relying and relied upon institutions are party to a tripartite agreement with a client, the notification is communicated during the initial exchange of documents.

5.128 RFIs relying upon third parties must also satisfy themselves that the third party consents to being relied upon. This consent should be in writing, and must confirm that, upon request by the relying RFI, the third party will make available, the RFI', copies of the verification data and other relevant documents or information on the customer, beneficial owner, and purpose and intended nature of the business relationship that the third party obtained when applying CDD measures.

5.129 Third parties are generally under no obligation to consent to be relied upon and may choose not to do so. In such circumstances, or if the RFI decides for any other reason that it does not wish to rely upon the third party, then the RFI must apply its own CDD measures to the customer.

Basis of reliance

5.130 RFIs should utilise a risk-based approach when determining the level of reliance that can be placed on the third party and the verification work the third party has carried out, and as a consequence, the amount of evidence that should be obtained directly from the customer.

5.131 In addition to satisfying itself that the third party meets the criteria of paragraph 5.121, RFIs should consider related risk factors, including:

- The regulatory and/or disciplinary record of the third party, to the extent that it is available;
- The nature of the customer, the product or service sought and the sums involved;
- Any adverse experience in business dealings with the third party and/or customer;

- Whether the third party has satisfactorily responded to any previous requests to make available, without delay, copies of the verification data it obtained when applying CDD measures;
- Any other knowledge, whether obtained at the outset of the relationship or subsequently, that the RFI has regarding the standing of the third party to be relied upon.

5.132 RFIs should also consider any geographic AML/ATF risks associated with the country or territory in which the third party is based and the degree to which the third party has effective measures in place to mitigate such risks. When the intermediary is located in a higher-risk jurisdiction, the business should not proceed unless the identity of the underlying customer and each beneficial owner has been verified to the satisfaction of the RFI providing the product or service.

5.133 RFIs must not rely upon any third party or enter into agency or correspondent arrangements where access to verification data without delay is likely to be impeded by confidentiality, secrecy, privacy or data protection restrictions.

5.134 For reliance to be permissible, relying RFIs should obtain certain information immediately, including:

- The identity of the customer;
- The identity of the beneficial owner;
- As appropriate, the purpose and intended nature of the business relationship; and
- The level of CDD that has been carried out.

5.135 In practice, at the outset of the customer relationship, and periodically throughout the customer relationship, RFIs will request, and promptly receive, copies of the documents, data and other information obtained by the third party for verification of the items listed above. This process is normally a part of an RFI's risk-based procedures for customer acceptance and on-going monitoring, and is generally set out in the form or forms that the relying RFI will require to be completed.

5.136 At a minimum, however, relying RFIs must satisfy themselves that copies of documents, data and other information used by the third party for verification of the items listed in paragraph 5.134 will be made available by the third party upon request, without delay, for at least five years following the latest transaction carried out by, for, or on behalf of a customer.

5.137 Periodically, and on a risk-sensitive basis, relying RFIs should test the willingness and ability of relied upon third parties to actually make available requested evidence of

verification. This is particularly relevant when on-going monitoring has identified a customer as high risk, when the third party is situated in, or a transaction involves, a high risk jurisdiction, or when knowledge or suspicion of money laundering or terrorism financing is present.

5.138 Where an RFI makes such a request and it is not met, the RFI will need to take account of that fact in its assessment of the third party in question, and of the risks associated with relying upon the third party in the future. In addition, the RFI should review its application of CDD in respect of the customer and/or beneficial owner(s) in question.

5.139 An RFI's AML/ATF policy statement should address the circumstances in which it may seek to rely upon a third party and how the RFI will assess whether the third party satisfies the requirements of this guidance. RFIs must also document the steps taken to confirm that a third party that is relied upon satisfies the requirements of this guidance. This is particularly important where the relied upon third party is situated in a country or territory other than Bermuda.

Group introductions

5.140 Where customers are introduced between different parts of the same financial sector group, entities that are part of the group may rely upon the identification and verification procedures conducted by that part of the group which first dealt with the customer, provided the following criteria are met:

- The group entity that carried out the CDD measures can be relied upon as a third party under this guidance;
- The group has implemented a group-wide AML/ATF programme;
- The group entity makes available to the group the information described paragraph 5.134;
- Foreign branches and majority owned subsidiaries of the group apply AML/ATF measures that are consistent with the group's home country AML/ATF requirements;
- The customer's relationship with the relying RFI requires an equal or lower level of CDD measures as compared to those actually applied by the relied upon institution; and
- The group's home is in Bermuda or in a jurisdiction that imposes equivalent AML/ATF requirements.

5.141 In such cases, one member of a group may confirm to another member of the group that the identity of the customer has been satisfactorily verified.

5.142 Where Bermuda RFIs have day-to-day access to all group customer information and records, and the identity of that customer has been verified previously to AML/ATF standards in

Bermuda, or in a jurisdiction that imposes equivalent AML/ATF requirements, there is no need to obtain a group introduction confirmation. However, if the identity of the customer has not been verified previously, for example because the group customer relationship pre-dates the introduction of AML/ATF regulations, or if the verification evidence is inadequate, any missing verification evidence will need to be obtained.

Use of pro-forma confirmations

5.143 For the purposes of paragraph 5.127, consent to be relied upon may be ascertained when an eligible third party under paragraph 5.121 provides a satisfactorily completed confirmation certificate. Pro-forma confirmation certificates for consent to be relied upon are attached to this guidance as **Annexes 5-I through 5-VI**.

Situations that are not reliance

A third party acting solely as an introducer

5.144 When a third party acts solely as an introducer between a customer and an RFI providing a product or service, and the introducer neither gives advice nor plays any part in the negotiation or execution of the transaction, all identification and verification obligations lie with the RFI providing the product or service. This does not preclude the introducing entity from carrying out identification and verification of the customer on behalf of the RFI providing the product or service, if the introducer is an agent for that RFI. For additional information, see paragraph 5.145.

A third party agent of the RFI providing a product or service

5.145 When a third party is an agent or appointed representative of the RFI providing the product or service, it is an extension of that RFI. Similarly, when the RFI providing the product or service has a direct sales force, that sales force is considered to be part of the RFI, whether or not it operates under a separate group legal entity. In such cases, the third party agent may obtain the appropriate verification evidence in respect of the customer, but the RFI providing the product or service is responsible for first specifying what should be obtained, and for ensuring that records of the verification evidence taken in respect of the customer are appropriately retained and accessible.

Regulated financial institutions

5.146 When a customer of a Bermuda RFI is an RFI under Regulation 10(2) and transacts solely on its own behalf, and not on behalf of any underlying customers, the Bermuda RFI's

measures to identify and verify the beneficial owner and intended nature of the business relationship may be reduced or largely eliminated.

5.147 When an RFI cannot apply simplified due diligence measures to a third party (see paragraphs 5.1 through 5.14), the RFI must apply standard, or as appropriate, enhanced, CDD measures to the third party and, where the third party acts for another and is not being relied upon, to the underlying customer.

Correspondent relationships

5.148 When a cross-border correspondent banking relationship exists or is being considered, in addition to conducting on-going monitoring and reporting any knowledge or suspicion of money laundering or terrorist financing, RFIs must:

- Determine from publically available information the nature of the respondent's business, its reputation and the quality of supervision, including whether it has been subject to an AML/ATF investigation or regulatory action;
- Assess the respondent's AML/ATF controls;
- Obtain approval from senior management before establishing new correspondent relationships (see paragraph 5.109);
- Clearly understand the respective responsibilities of each institution; and
- With respect to "payable-through accounts", be satisfied that the respondent has conducted CDD on the customers having direct access to the accounts of the Bermuda RFI, and that the respondent is able to provide relevant CDD information to the RFI, upon request and in accordance with paragraph 5.134 of this guidance.

Outsourcing

5.149 An outsourcing arrangement occurs where an RFI uses a service provider to perform an activity, such as applying CDD measures that would normally be carried out by the RFI. Irrespective of whether the service provider is in Bermuda or overseas, and irrespective of whether the service provider is within or independent of any financial sector group of which the RFI may be a member, any outsourcing arrangement is subject to the Regulations and these Guidance Notes.

5.150 Outsourced activities should be carried out in accordance with the RFI's procedures and the RFI should have effective control over the service provider's implementation of those procedures. An RFI's board or similarly empowered body or individual, such as the Compliance Officer, should establish clear accountability for all outsourced activities, as if the activities were performed in-house according to the RFI's own standards of internal control and oversight.

5.151 In any outsourcing arrangement, an RFI cannot contract out of its statutory and regulatory responsibilities to prevent and detect ML/TF.

5.152 Where an RFI outsources an activity to a service provider, the RFI remains responsible at all times for compliance with the Regulations and these Guidance Notes.

5.153 In any outsourcing relationship, the RFI should take care to avoid:

- Impeding the effective ability of the RFI's senior management to monitor and manage the RFI's compliance functions, including the application of non-standard measures, such as enhanced due diligence;
- Impeding the effective ability of the RFI's board or similarly empowered body or individual to provide oversight;
- Impeding the effective ability of the appropriate regulator to monitor the RFI's compliance with all obligations under the regulatory system;
- Reducing the responsibility of the Bermuda RFI and/or its managers and officers;
- Removing or modifying any conditions subject to which the firm's authorisation was granted; and
- Increasing ML/TF risk in any way that is not adequately addressed through appropriate risk assessment and mitigation.

5.154 RFIs must not enter into outsourcing arrangements where access to data without delay is likely to be impeded by confidentiality, secrecy, privacy, or data protection restrictions.

Functions that cannot be outsourced

5.155 In any outsourcing relationship the RFI should retain in-house the resources and expertise necessary to:

- Set the RFI's risk policies and procedures;
- Continuously identify, assess, monitor and manage the risks associated with outsourcing activities to the service provider;

- Continuously supervise, monitor and test the adequacy of the activities carried out by the service provider; and
- Ensure the RFI's ability to resume direct control over the outsourced activity in the event that a need arises.

Risk management

5.156 Both prior to entering into and throughout any outsourcing arrangement, an RFI should identify and assess the risks created by outsourcing the proposed activities. In particular, an RFI should assess whether and how outsourcing may affect its ability to fulfil its obligations under the Regulations and these Guidance Notes. Where all risks identified and assessed can be effectively and appropriately mitigated, those risks should be mitigated. Where all risks identified and assessed cannot be effectively mitigated, an RFI should not enter into the outsourcing arrangement.

5.157 RFIs that enter into any outsourcing arrangement should establish key performance measures for the outsourced activities and for the service provider itself. RFIs should regularly assess the service provider's performance against those measures and include the findings of such assessments as a standing agenda point in managerial and operational risk meetings.

5.158 Outsourcing RFIs should plan and implement a policy to maintain the continuity of their business in the event that the provision of services by a service provider fails or deteriorates to an unacceptable degree. The policy should include contingency planning and a clearly defined strategy for exiting the outsourcing arrangement.

Due diligence on the service provider

5.159 RFIs considering an outsourcing arrangement should carry out due diligence as to the service provider under consideration. The purpose of the due diligence is to determine whether the service provider has the ability, capacity, and any required authorisation to perform the outsourced activities reliably, professionally, and in accordance with the Regulations and these Guidance Notes. RFIs should establish a written policy concerning the scope and frequency of initial and on-going due diligence carried out as to such service providers.

5.160 At a minimum, RFIs carrying out due diligence as to a service provider should consider the following:

- Whether the service provider is licensed or otherwise authorised to carry out the outsourced activities;
- Whether, where required, the service provider is effectively regulated;
- Whether any operational, financial, human resource, structural, legal, or regulatory considerations may affect the service provider's ability to carry out the outsourced activities or impede the RFI's constant and ready access to relevant information held by the service provider, including customer and transaction information;
- Whether the service provider has in place contingency plans in the event of operational, financial, human resource, structural, legal, or regulatory considerations that negatively impact the service provider's ability to carry out the outsourced activities;
- Whether any confidentiality, secrecy, privacy, or data protection restrictions may impede the RFI or any relevant Bermuda regulatory authorities from effectively monitoring the activities of the service provider; and
- Whether the service provider has in place effective procedures to back up and protect the data of the RFI and its customers, and to quickly identify any data breaches.

5.161 In determining whether the use of a service provider outside of Bermuda is appropriate, RFIs should conduct enhanced due diligence to evaluate their ability to effectively monitor the foreign service provider, maintain the confidentiality of firm and client information, and execute contingency plans and exit strategies.

Outsourcing agreement

5.162 An RFI should draft and, subject to paragraphs 5.162 through 5.174, execute with the service provider a comprehensive, written, and legally binding agreement governing the outsourcing arrangement. The outsourcing agreement should normally be governed by Bermuda law. If not governed by Bermuda law, the agreement should be governed by the law of a jurisdiction that imposes equivalent AML/ATF requirements.

Clear statement of functions to be outsourced

5.163 The outsourcing agreement should be drafted such that it removes any doubt as to each entity's roles and responsibilities and the exposure each entity faces in the event of an operational issue.

5.164 The outsourcing agreement should:

- Precisely define the rights and obligations of the RFI and the service provider;

- Specify all activities being outsourced;
- Clearly state all requirements, including regulatory obligations, concerning the service provider's performance of the outsourced activities;
- Specify the persons at both the RFI and the service provider who are responsible for implementing, monitoring, and managing the outsourcing arrangement; and
- Specifically state the name or title of the RFI's Bermuda officer who retains ultimate responsibility for the RFI's compliance with the Regulations and these Guidance Notes. This person is normally the Compliance Officer referred to in paragraph 1.36 of these guidance notes.

Monitoring

5.165 The outsourcing agreement should establish qualitative and quantitative performance standards to enable the RFI to assess the adequacy of service provision. The agreement should also authorise and require the RFI to continuously monitor and assess the service provider against the established performance standards in order to ensure that any necessary corrective measures are taken promptly. The level of monitoring, assessment, inspection, and auditing required by the agreement should be proportionate to the risks involved and the size and complexity of the outsourced activity.

5.166 At a minimum, the outsourcing agreement should ensure that:

- The service provider is required to report regularly to the RFI;
- The RFI has on- and off-site access to all information required to monitor and assess the service provider's performance, including access requisite for the purposes of conducting an audit of the outsourced activities;
- The service provider is required to promptly disclose to the RFI any operational, financial, human resource, structural, legal, or regulatory development that may affect the service provider's ability to carry out the outsourced activities in compliance with the Regulations and these Guidance Notes;
- The service provider is required to promptly notify the RFI of any change that may impede the RFI's complete, constant, and unfettered access to relevant information held by the service provider, including customer and transaction information;

Access to information

5.167 For the purposes of complying with the Regulations and these Guidance Notes and to respond to lawful requests from regulatory and law enforcement authorities, the outsourcing agreement should oblige the service provider to allow the RFI's specified persons complete, constant, and unfettered access to all data relating to the outsourced activity. The agreement

should also grant the RFI's external auditors full and unrestricted rights of inspection and auditing of that data.

5.168 The outsourcing agreement should require the service provider to allow the outsourcing RFI's supervisory authority direct access to relevant data and the service provider's premises as required for the purposes of supervision and inspection. Where outsourcing to service providers abroad, the Bermuda RFI is responsible for ensuring that the supervisory authority can exercise its information gathering rights, including its right to demand documents and audits, and, as compatible with the overarching legal framework, its inspection rights.

Data protection

5.169 The outsourcing agreement should require the service provider to maintain appropriate procedures to back up and ensure the protection of confidential information. The agreement should require the service provider to immediately disclose to the RFI any suspected or confirmed data breach.

Contingency planning and exit strategy

5.170 The outsourcing agreement should expressly permit the Bermuda RFI to take remedial action where the service provider's performance falls short of that required by the outsourcing agreement, the Regulations, or these Guidance Notes or where a Bermuda regulatory authority orders the Bermuda RFI in writing to do so.

5.171 The outsourcing agreement should entitle the RFI to terminate the outsourcing arrangement where the service provider undergoes a change of control, becomes insolvent, goes into liquidation or receivership, or for any reason materially fails to perform according to the outsourcing agreement, the Regulations, and these Guidance Notes.

5.172 The outsourcing agreement should require the RFI and the service provider to establish, implement, and maintain a contingency plan for disaster recovery and for periodic testing of backup facilities to understand recovery times and to ensure the continuity of the outsourced activity.

5.173 The outsourcing agreement should include a termination and exit management clause that allows the outsourced activities and any related data to be transferred to another service provider or to be reincorporated into the outsourcing RFI. Care should be taken to ensure that any termination of an outsourcing arrangement is carried out without detriment to the continuity and quality of the provision of services to clients.

Subcontracting

5.174 Any subcontracting arrangement should be detailed in the outsourcing agreement. If the outsourcing agreement allows the service provider to subcontract any of the activities to be outsourced, any subcontractor should be subject to the same levels of due diligence as the primary service provider. Additionally, any subcontractor should be required to adhere to all aspects of the outsourcing agreement and to the outsourcing RFI's responsibilities under the Regulations and these Guidance Notes. The outsourcing RFI should be required to approve in writing any changes to the subcontracting arrangements.

ANNEX 5-I

CONFIRMATION OF VERIFICATION OF IDENTITY PRIVATE INDIVIDUAL

INTRODUCTION BY A BERMUDA AML/ATF REGULATED FINANCIAL INSTITUTION

1: DETAILS OF INDIVIDUAL (see explanatory notes below)

Full legal name of Customer (and any former names and other names used):	
Current Address (and previous address if the address has changed in the last three months):	
Date and Place of Birth:	
Nationality:	
Gender:	
Government-issued Personal Identification Number: (e.g. Passport, National Identity Card or Driving Licence)	

2: CONFIRMATION

We confirm that

(a) The information in section 1 above was obtained by us in relation to the customer;

(b) The evidence we have obtained to verify the identity of the customer meets the requirements of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008, and any relevant authoritative guidance provided in relation to the type of business or transaction to which this confirmation relates, including, but not limited to Chapter 4 and paragraphs 5.118 through 5.148 of the 2016 Guidance Notes for AML/ATF Regulated Financial Institutions on Anti-Money Laundering and Anti-Terrorist Financing;

(c) We consent to your reliance upon us for the provision of relevant customer records; in the event of any enquiry from you, copies of the relevant customer records will be made available without delay, for a period of at least five years following the date the business relationship ends or, in the case of an occasional transaction, five years beginning on the date on which the transaction is completed carried out by, for, with or on behalf of the customer;

(d) Information regarding the purpose and intended nature of the business relationship is

being provided in connection with this confirmation; and

(e) The customer information was obtained using a (choose one) standard ☐ or enhanced ☐ level of customer due diligence.

Signed:	
Name:	
Position:	
Date:	

3: DETAILS OF INTRODUCING FIRM

Name of Licensed	
Jurisdiction:	
Name of	
Regulator	

Explanatory notes

1: A separate confirmation must be completed for each customer and where a third party is involved, the identity of that person must also be verified, and a confirmation provided.

2: This form cannot be used to verify the identity of any customer whose identity has not been verified as a result of being an existing customer of the introducing firm where the standard of verification did not meet the verification standards in the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008..

3: This form cannot be used to confirm verification when the introducing firm has relied upon any firm other than a member of the introducing firm's financial sector group to verify the customer's identify.

4: This form cannot be used to verify the identity of any customer for whom simplified customer due diligence measures were applied.

ANNEX 5-II

CONFIRMATION OF VERIFICATION OF

IDENTITY PRIVATE INDIVIDUAL

INTRODUCTION BY A FINANCIAL INSTITUTION LOCATED IN A COUNTRY OR TERRITORY OTHER THAN BERMUDA

(which the receiving firm has accepted as being regulated, supervised or monitored for, and having measures in place for compliance with AML/ATF regulations equivalent to those of Bermuda)

1: DETAILS OF INDIVIDUAL (see explanatory notes below)

Full legal name of Customer (and any former names and other names used):	
Current Address (and previous address if the address has changed in the last three months):	
Date and Place of Birth:	
Nationality:	
Gender:	
Government-issued Personal Identification Number: (e.g. Passport, National Identity Card or Driving Licence)	

2: CONFIRMATION

We confirm that

(a) The information in section 1 above was obtained by us in relation to the customer;

(b) The evidence we have obtained to verify the identity of the customer meets the requirements of local law and regulation, and any relevant authoritative guidance provided in relation to the type of business or transaction to which this confirmation relates;

(c) We consent to your reliance upon us for the provision of relevant customer records; in the event of any enquiry
from you, copies of the relevant customer records will be made available without delay, for a period of at least five years following the date the business relationship ends or, in

the case of an occasional transaction, five years beginning on the date on which the transaction is completed carried out by, for, with or on behalf of the customer

(d) Information regarding the purpose and intended nature of the business relationship is being provided in connection with this confirmation; and

(e) The customer information was obtained using a (choose one) standard ☐ or enhanced ☐ level of customer due diligence.

Signed:	
Name:	
Position:	
Date:	

3: DETAILS OF INTRODUCING FIRM

Name of Licensed	
Jurisdiction:	
Name of	
Regulator License	

Explanatory notes

1: A separate confirmation must be completed for each customer and where a third party is involved, the identity of that person must also be verified, and a confirmation provided.

2: This form cannot be used to verify the identity of any customer whose identity has not been verified as a result of being an existing customer of the introducing firm where the standard of verification did not meet the verification standards in the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008..

3: This form cannot be used to confirm verification when the introducing firm has relied upon any firm other than a member of the introducing firm's financial sector group to verify the customer's identify.

4: This form cannot be used to verify the identity of any customer for whom simplified customer due diligence measures were applied.

ANNEX 5-III

CONFIRMATION OF VERIFICATION OF IDENTITY
CORPORATE AND OTHER NON-PERSONAL ENTITY
INTRODUCTION BY A BERMUDA AML/ATF REGULATED FINANCIAL INSTITUTION

1: DETAILS OF CUSTOMER (see explanatory notes below)

Full name of Customer (and any trade names):	
Date and Place of Incorporation (or registration or establishment):	
Location of Business (full operating address):	
Registered office in country of incorporation:	
Type of Entity (corporate, trust, etc)**:**	
Official Identification Number (where applicable)**:**	
Relevant Company Registry, Regulator and/ or Market Listing Authority:	
Name and Date of Birth of Each Director (or equivalent):	
Name and Date of Birth of Each Beneficial Owner (or equivalent)**:**	

2: CONFIRMATION

We confirm that

(a) The information in section 1 above was obtained by us in relation to the customer;

(b) The evidence we have obtained to verify the identity of the customer meets the requirements of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008, and any relevant authoritative guidance provided in relation to the type of business or transaction to which this confirmation relates, including, but not limited to Chapter 4 and paragraphs 5.118 through 5.148 of the 2016 Guidance Notes for AML/ATF Regulated Financial Institutions on Anti-Money

Laundering and Anti-Terrorist Financing;

(c) We consent to your reliance upon us for the provision of relevant customer records; in the event of any enquiry from you, copies of the relevant customer records will be made available without delay, for a period of at least five years following the date the business relationship ends or, in the case of an occasional transaction, five years beginning on the date on which the transaction is completed carried out by, for, with or on behalf of the customer;

(d) Information regarding the ownership and control structure of the customer, and the purpose and intended nature of the business relationship is being provided in connection with this confirmation; and

(e) The customer information was obtained using a (choose one) standard ☐ or enhanced ☐ level of customer due diligence.

Signed:	
Name:	
Position:	
Date:	

3: DETAILS OF INTRODUCING FIRM

Name of Licensed	
Business Address:	
Name of	
Regulator	

Explanatory notes

1: "Relevant company registry" includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.

2: "Beneficial owner" includes each person that effectively owns or controls more than 25% of a customer's funds, assets or voting rights.

3: This form cannot be used to verify the identity of any customer whose identity has not been verified as a result of being an existing customer of the introducing firm where the standard of verification did not meet the verification standards in the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008..

4: This form cannot be used to confirm verification when the introducing firm has relied upon any firm other than a member of the introducing firm's financial sector group to verify the customer's identify.

5: This form cannot be used to verify the identity of any customer for whom simplified customer due diligence measures were applied.

6: Where the number of directors, signatories and other persons exercising control over management of the corporate is high, RFIs may use a risk-based approach to

determine whose identity to verify (Paragraph 4.88).

ANNEX 5-IV

CONFIRMATION OF VERIFICATION OF IDENTITY

CORPORATE AND OTHER NON-PERSONAL ENTITY

INTRODUCTION BY A FINANCIAL INSTITUTION LOCATED IN A COUNTRY OR TERRITORY OTHER THAN BERMUDA

(which the receiving firm has accepted as being regulated, supervised or monitored for, and having measures in place for compliance with AML/ATF regulations equivalent to those of Bermuda)

1: DETAILS OF CUSTOMER (see explanatory notes below)

Full name of Customer (and any trade names):	
Date and Place of Incorporation (or registration or establishment):	
Location of Business (full operating address):	
Registered office in country of incorporation:	
Type of Entity (corporate, trust, etc.)**:**	
Official Identification Number (where applicable)**:**	
Relevant Company Registry, Regulator and/ or Market Listing Authority:	
Name and Date of Birth of Each Director (or equivalent)**:**	
Name and Date of Birth of Each Beneficial Owner (or equivalent)**:**	

2: CONFIRMATION

We confirm that

(a) The information in section 1 above was obtained by us in relation to the customer;

(b) The evidence we have obtained to verify the identity of the customer meets the requirements of local law and regulation, and any relevant authoritative guidance provided in relation to the type of business or transaction to which this confirmation relates;

(c) We consent to your reliance upon us for the provision of relevant customer records; in

the event of any enquiry
from you, copies of the relevant customer records will be made available without delay, for a period of at least five years following the date the business relationship ends or, in the case of an occasional transaction, five years beginning on the date on which the transaction is completed carried out by, for, with or on behalf of the customer.

(d) Information regarding the ownership and control structure of the customer, and the purpose and intended nature of the business relationship is being provided in connection with this confirmation; and

(e) The customer information was obtained using a (choose one) standard ☐ or enhanced ☐ level of customer due diligence.

Signed:	
Name:	
Position:	
Date:	

3: DETAILS OF INTRODUCING FIRM

Name of Licensed	
Business Address:	
Name of	
Regulator	

Explanatory notes

1: "Relevant company registry" includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.

2: "Beneficial owner" includes each person that effectively owns or controls more than 25% of a customer's funds, assets or voting rights.

3: This form cannot be used to verify the identity of any customer whose identity has not been verified as a result of being an existing customer of the introducing firm where the standard of verification did not meet the verification standards in the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008..

4: This form cannot be used to confirm verification when the introducing firm has relied upon any firm other than a member of the introducing firm's financial sector group to verify the customer's identify.

5: This form cannot be used to verify the identity of any customer for whom simplified customer due diligence measures were applied.

6: Where the number of directors, signatories and other persons exercising control over

management of the corporate is high, RFIs may use a risk-based approach to determine whose identity to verify (Paragraph 4.88).

ANNEX 5-V

CONFIRMATION OF VERIFICATION OF IDENTITY

GROUP INTRODUCTION

PRIVATE INDIVIDUAL

1: DETAILS OF INDIVIDUAL (see explanatory notes below)

Full legal name of Customer (and any former names and other names used):	
Current Address (and previous address if the address has changed in the last three months):	
Date and Place of Birth:	
Nationality:	
Gender:	
Government-issued Personal Identification Number: (e.g. Passport, National Identity Card or Driving Licence)	

2: CONFIRMATION

We confirm that

(a) The information in section 1 above was obtained by us in relation to the customer;

(b) The evidence we have obtained to verify the identity of the customer meets the requirements of:

i. The Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008, and any relevant authoritative guidance provided in relation to the type of business or transaction to which this confirmation relates, including, but not limited to Chapter 4 and paragraphs 5.118 through 5.148 of the 2016 Guidance Notes for AML/ATF Regulated Financial Institutions on Anti-Money Laundering and Anti-Terrorist Financing; and/or

ii. Local law and regulation, and any relevant authoritative guidance provided in relation to the type of business or transaction to which this confirmation relates;

(c) We consent to your reliance upon us for the provision of relevant customer records; in the event of any enquiry from you, copies of the relevant customer records will be made available without delay, for a period of at least five years following the date the business relationship ends or, in the case of an occasional transaction, five years

beginning on the date on which the transaction is completed carried out by, for, with or on behalf of the customer;

(d) Information regarding the purpose and intended nature of the business relationship is being provided in connection with this confirmation; and

(e) The customer information was obtained using a (choose one) standard ☐ or enhanced ☐ level of customer due diligence.

Signed:	
Name:	
Position:	
Date:	

3: DETAILS OF GROUP FIRM

Name of Licensed entity:	
Relationship to receiving entity:	
Business address:	
Jurisdiction:	
Registered number (if applicable):	
Group's home jurisdiction:	

Explanatory notes

1: A separate confirmation must be completed for each customer and where a third party is involved, the identity of that person must also be verified, and a confirmation provided.

2: This form cannot be used to verify the identity of any customer whose identity has not been verified as a result of being an existing customer of the introducing firm where the standard of verification did not meet the verification standards in the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008..

3: This form cannot be used to confirm verification when the introducing firm has relied upon any firm other than a member of the introducing firm's financial sector group to verify the customer's identify.

4: This form cannot be used to verify the identity of any customer for whom simplified

customer due diligence measures were applied.

ANNEX 5-VI

CONFIRMATION OF VERIFICATION OF IDENTITY
GROUP INTRODUCTION
CORPORATE AND OTHER NON-PERSONAL ENTITY

1: DETAILS OF CUSTOMER (see explanatory notes below)

Full name of Customer (and any trade names):	
Date and Place of Incorporation (or registration or establishment):	
Location of Business (full operating address):	
Registered office in country of incorporation:	
Type of Entity (corporate, trust, etc.)**:**	
Official Identification Number	
Relevant Company Registry, Regulator and/ or Market Listing Authority:	
Name and Date of Birth of Each Director (or equivalent):	
Name and Date of Birth of Each Beneficial Owner (or equivalent)**:**	

2: CONFIRMATION

We confirm that

(a) The information in section 1 above was obtained by us in relation to the customer;

(b) The evidence we have obtained to verify the identity of the customer meets the requirements of:

i. The Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008, and any relevant authoritative guidance provided in relation to the type of business or transaction to which this confirmation relates, including, but not limited to Chapter 4 and paragraphs 5.118 through 5.148 of the 2016 Guidance Notes for

AML/ATF Regulated Financial Institutions on Anti-Money Laundering and Anti-Terrorist Financing; and/or

ii. Local law and regulation, and any relevant authoritative guidance provided in relation to the type of business or transaction to which this confirmation relates;

(c) We consent to your reliance upon us for the provision of relevant customer records; in the event of any enquiry from you, copies of the relevant customer records will be made available without delay, for a period of at least five years following the date the business relationship ends or, in the case of an occasional transaction, five years beginning on the date on which the transaction is completed carried out by, for, with or on behalf of the customer;

(d) Information regarding the ownership and control structure of the customer, and the purpose and intended nature of the business relationship is being provided in connection with this confirmation; and

(e) The customer information was obtained using a (choose one) standard ☐ or enhanced ☐ level of customer due diligence.

Signed:	
Name:	
Position:	
Date:	

3: DETAILS OF GROUP FIRM

Name of Licensed entity:	
Relationship to receiving entity:	
Business address:	
Jurisdiction:	
Registered number (if applicable):	
Group's home jurisdiction:	

Explanatory notes

1: "Relevant company registry" includes other registers, such as those maintained by charity commissions (or equivalent) or chambers of commerce.

2: "Beneficial owner" includes each person that effectively owns or controls more than 25% of a customer's funds, assets or voting rights.

3: This form cannot be used to verify the identity of any customer whose identity has not been verified as a result of being an existing customer of the introducing firm where the standard of verification did not meet the verification standards in the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008..

4: This form cannot be used to confirm verification when the introducing firm has relied upon any firm other than a member of the introducing firm's financial sector group to verify the customer's identify.

5: This form cannot be used to verify the identity of any customer for whom simplified customer due diligence measures were applied.

6: Where the number of directors, signatories and other persons exercising control over management of the corporate is high, RFIs may use a risk-based approach to determine whose identity to verify (Paragraph 4.88).

CHAPTER 6 - INTERNATIONAL SANCTIONS

Introduction

6.1 This chapter provides guidance to assist RFIs in meeting their obligations under the Bermuda sanctions regime.

6.2 The obligations of RFIs with respect to international sanctions are set forth primarily in the International Sanctions Act 2003, the International Sanctions Regulations 2013, the Banks and Deposit Companies Act 1999 and Regulation 11 of the Proceeds of Crime Regulations 2008.

6.3 RFIs should make their sanctions compliance programme an integral part of their AML/ATF compliance programme, subject to several key differences described in this chapter.

6.4 The guidance provided in this chapter is not exhaustive. Although this guidance focuses on financial sanctions and asset freezes, RFIs must also be aware of the nature and requirements of other types of sanctions measures. It is the responsibility of each entity to put in place policies, procedures and controls that ensure compliance with the Bermuda sanctions regime.

Overview of international sanctions

6.5 Sanctions are enforcement measures implemented for political reasons by countries and international organisations to maintain or restore international peace and security. The principal purpose of sanctions is usually to change the behaviour of the individual, group, company, organisation, industry or political regime that is targeted by the sanction. Numerous different sanctions may be in effect at any given time. Most sanctions include information as to why they have been imposed and what their aim is.

6.6 Measures that are frequently applied through international sanctions include:

- Financial sanctions, including asset freezes and investment bans;
- Trade controls on the importation, exportation or financing of specified goods, services, equipment and activities;

- Embargoes on the sale, export or supply of weaponry and related materials, training, technical assistance and financing; and
- Travel bans on named individuals.

6.7 The primary sources of international sanctions affecting Bermuda RFIs are the United Nations and the European Union. For reference, see the sanctions pages at www.un.org and eeas.europa.eu. Some countries, however, also impose unilateral sanctions. For more information, see paragraphs 6.12 through 6.14.

Penalties for non-compliance

6.8 The Bermuda sanctions regime requires absolute compliance. Any person breaching an obligation under the Bermuda sanctions regime, without a successful defence, will be guilty of an offence punishable by imprisonment for up to seven years or a fine, or both.

6.9 Regulation 11 of the Proceeds of Crime Regulations 2008 requires RFIs to apply enhanced due diligence to persons and transactions involving international sanctions. The Banks and Companies Act of 1999 establishes that any failure to comply with the Bermuda sanctions regime implicates the fundamental determination of whether an RFI is operating in a prudent manner. As a result, any violation of the Bermuda sanctions regime is also a regulatory matter that may result in the BMA cancelling an RFI's registration, publicly censuring the RFI and imposing civil fine of up to $500,000.

6.10 RFIs must be aware that, in contrast to AML/ATF measures, which generally permit firms to set their own timetables for verifying and updating CDD information, an RFI risks breaching a sanctions obligation as soon as a person, entity or good is listed under a sanctions regime in effect in Bermuda. In addition, whereas an RFI may choose to transact with a higher-risk individual or entity, it may not transact with any individual or entity subject to the Bermuda sanctions regime without first applying for and obtaining an appropriate license.

6.11 The Bermuda sanctions regime applies to individuals as well as legal persons and arrangements. Where any RFI is guilty of an offence, and that offence is proved to have been committed with the consent of, connivance of, or to be attributable to any neglect on the part of any director, manager, secretary or other similar officer of the RFI, or any person who was purporting to act in any such capacity, that

person, as well as the RFI, is guilty of that offence and is liable to be proceeded against and punished accordingly.

Non-Bermudian sanctions obligations

6.12 Where an RFI has a presence or is otherwise active in a jurisdiction outside of Bermuda, it may be required to comply with the sanctions requirements of that other jurisdiction. Transacting with a customer or counterparty in another jurisdiction may also trigger the sanctions requirements of that jurisdiction, even if an RFI has no presence there.

6.13 RFIs should obtain legal advice to understand which sanctions regimes apply to which aspects of their business and to ensure that they correctly comply with applicable sanctions while not incorrectly applying sanctions regimes of other jurisdictions to Bermuda business.

6.14 Where an RFI operates in a number of jurisdictions, a consistent group policy should be established to assist local business units in ensuring that their local procedures meet minimum group standards while also complying with local requirements. For additional information on group policies, see paragraphs 1.57 through 1.69.

The Bermuda sanctions regime

6.15 Most of Bermuda's international sanctions are brought into force through the International Sanctions Act 2003 and the International Sanctions Regulations 2013.

6.16 The Bermuda sanctions regime is based largely upon the United Kingdom's sanctions regime. The International Sanctions Act 2003 grants the Minister of Legal Affairs authority to make regulations giving effect to any international sanctions obligation of the United Kingdom. The International Sanctions Regulations 2013 are made pursuant to that authority.

6.17 Schedule 1 of the International Sanctions Regulations 2013 lists the United Kingdom's sanctions-related Overseas Territories Orders in Council ("Orders") that have been brought into force in Bermuda.

6.18 The Minister of Legal Affairs amends Schedule 1 of the International Sanctions Regulations 2013 by regulation to ensure that new sanctions are brought into force in Bermuda and sanctions, once withdrawn in the United Kingdom, are retired from effect in Bermuda. Schedule 2 lists sanctions that have been revoked.

6.19 A portal to Orders in force in Bermuda and lists of "designated" or "listed" persons and "restricted goods" is available at www.namlc.bm.

6.20 The details of each sanction regime in effect in Bermuda are contained in one or more of the following texts:

- The United Kingdom's sanctions-related Orders;
- HM Treasury's list of Current Arms Embargoes and Other Restrictions;
- HM Treasury's Consolidated List of Targets;
- Schedule 2 to the United Kingdom Export Control Order 2008;
- The European Union's Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions;
- The Common Military List of the European Union; and
- The relevant annexes to the relevant European Union regulations.

6.21 The scope of restrictions contained in each Order varies and the Order itself, together with any accompanying lists, annexes, schedules, updates or amendments, is controlling. However, most of the Orders provide for most or all of the following common restrictions:

- Asset freezing;
- Reporting;
- Information gathering; and
- Licensing.

6.22 An asset freeze generally prohibits dealings with the funds or economic resources that are owned, held or controlled by a sanctions target. An asset freeze may also prohibit making funds, economic resources and in some cases, financial services available, directly or indirectly, to or for the benefit of a sanctions target. Asset freezing can therefore affect any transaction or business relationship in which a customer, counterparty, beneficial owner, trustee or other party is a sanctions target or is acting on behalf of or for the benefit of a sanctions target.

6.23 Asset freezes generally apply to funds and assets, broadly defined, that are:

- Held in the name of a sanctions target;
- Held for the benefit of a sanctions target;
- Received from the sanctions target, either directly or indirectly; and
- Destined for the sanctions target or for the benefit of the sanctions target either directly or indirectly.

6.24 Indirect payments are those made to someone acting on behalf of a sanctions target. A payment that is for the benefit of a sanctions target is a payment that is made to a third party to satisfy an obligation of a sanctions target.

6.25 Sanctions in effect in Bermuda require RFIs to inform the Governor of any instance in which:

- The RFI knows or suspects that a customer or any person with whom the RFI has had dealings is a sanctions target; or
- The RFI or sanctions target has breached a sanction.

6.26 Any report described in paragraph 6.25 must be made to the Governor, and a copy should be provided to the BMA. For additional information about sanctions-related reporting, see paragraphs 6.74 through 6.76.

6.27 Sanctions in effect in Bermuda also grant authorised officers, such as police officers, a package of information gathering powers. These powers often include, among other things, establishing the nature of any financial transactions entered into by a sanctions target, conducting investigations of potential violations of the sanctions regime, copying documents and requesting officers of RFIs to give an explanation of documents.

6.28 The Governor has the sole authority to grant a license to an RFI to engage in an activity that would otherwise be prohibited by a sanctions regime. For additional information about licensing, see paragraphs 6.79 through 6.81.

Compliance with the Bermuda sanctions regime

6.29 Each RFI must have adequate policies, procedures and controls to comply with the Bermuda sanctions regime.

6.30 An RFI's policies, procedures and controls should be documented, and should be reviewed and endorsed by senior management.

6.31 Each RFI's policies, procedures and controls must enable it to screen its customers and transactions to determine whether it is conducting or may conduct business involving any sanctioned person, entity, activity or good.

6.32 The RFI's sanctions checking processes should be proportionate to the nature and size of its business, and should be likely to identify all true matches with sanctions targets. For additional information on true matches, see paragraphs 6.70 through 6.72.

6.33 An RFI's process of determining which sanctions compliance measures are proportionate and likely to identify all true matches differs in a key way from the risk-based approach for AML/ATF compliance described in **Chapter 2**. Whereas an RFI may choose to have a higher risk tolerance with regard to AML/ATF compliance and therefore may choose to transact with higher-risk customers, an RFI may not choose to transact in violation of the Bermuda sanctions regime. There is therefore no room for risk tolerance in sanctions compliance. Any RFI that provides any funds or financial services to a sanctions target or fails to freeze the assets of a sanctions target, without a proper license from the Governor, is in breach of the sanctions regime and liable to be prosecuted.

6.34 To tailor its sanctions compliance measures to the nature and size of its business, an RFI should take the following steps:

- Understand and identify the applicable sanctions;
- Assess the RFI's exposure to sanctioned persons, entities and activities;
- Develop and document appropriate policies, procedures and controls in order to comply with the sanctions;
- Apply the sanctions compliance policies, procedures and controls that have been developed and documented;
- Maintain sanctions information up to date; and
- Regularly review, test and improve the sanctions compliance policies, procedures and controls put in place.

6.35 Each RFI should ensure that its sanctions-related policies, procedures and controls effectively guide the RFI in:

- Ensuring up-to-date knowledge of the applicable sanctions;
- Tailoring sanctions compliance measures to the RFI's business;
- Screening the RFI's customers, transactions, third party service providers and geographic connections for potential matches with sanctions targets;
- Reviewing potential matches to identify true matches;
- Freezing assets or taking any other required action in the event of a true match;
- Reporting true matches and any breaches;
- Applying for and monitoring compliance with licenses;
- Ensuring appropriate staff awareness and training;
- Documenting and recording actions taken to comply with the sanctions regime, and the rationale for each such action; and
- Reviewing the effectiveness of the RFI's policies, procedures and controls.

6.36 To ensure up-to-date knowledge of the applicable sanctions, an RFI should have regard to the sources of information noted in paragraph 6.20, and should obtain regular updates via an email or subscription service. As an initial step, each RFI should refer to HM Treasury's Consolidated List of Targets and to the lists of restricted goods, both of which are linked at www.namlc.bm.

6.37 RFIs should bear in mind that HM Treasury's Consolidated List of Targets and the lists of restricted goods linked at www.namlc.bm may identify targets of sanctions that are not in effect in Bermuda. Where an RFI identifies a true match with a sanctions target on one of the lists, the RFI should verify whether the particular sanction regime under which the target is listed appears in Schedule 1 of the International Sanctions Regulations 2013. For additional information about reporting matches, see paragraphs 6.74 through 6.76.

6.38 Each RFI must ensure that it knows its business and does not breach the sanctions regime. To reduce the likelihood of breaching the sanctions regime, RFIs should focus their compliance resources on areas of their business that carry a greater likelihood of involvement with sanctions targets. However, RFIs cannot ignore areas of their business that are less likely to involve sanctions targets. RFIs must ensure that their sanctions-related policies, procedures and controls also address business areas in which dealings with a sanctions target are unlikely but possible.

6.39 Screening customers and transactions for potential matches with sanctions targets is addressed in paragraphs 6.52 through 6.69.

6.40 Reviewing potential matches to identify true matches, and reporting true matches and any breaches are addressed in paragraphs 6.70 through 6.76.

6.41 RFIs must ensure that they have policies, procedures and controls in place to take any action required by an applicable sanction. Required actions are contained in each Order and any accompanying lists, annexes, schedules, updates or amendments. As stated in paragraph 6.22, requirements to freeze funds and assets generally apply not only to customers but also to any other person or entity involved in a transaction. Asset freezing can therefore affect any transaction or business relationship in which a customer, counterparty, beneficial owner, trustee or other party is a sanctions target, or is acting on behalf of or for the benefit of a sanctions target.

6.42 Applying for and monitoring compliance with licenses is addressed in paragraphs 6.79 through 6.81.

6.43 RFIs should ensure that effective policies, procedures and controls are implemented to prohibit and detect attempts by employees or customers to:

- Omit, delete or alter information in payment messages for the purpose of avoiding detection of that information by other payment service providers in the payment chain; or
- Structure transactions for the purpose of concealing the involvement of a sanctions target.

Training

6.44 Each RFI should put in a place a sanctions-related employee training and awareness programme that is appropriate for the RFI's business.

6.45 The form, structure and scope of an RFI's training and awareness programme should be in line with the guidance provided **in Chapter 10: Employee Training and Awareness**, bearing in mind the differences between complying with AML/ATF obligations and sanctions obligations.

6.46 The substance of the training and awareness programme should, at a minimum, include the RFI's policies, procedures and controls for:

- Complying with new sanctions that come into force;
- Ceasing compliance with sanctions that have been retired from effect;
- Screening for applicable sanctions targets;
- Reporting true matches and any breaches;
- Documenting actions taken to comply with the sanctions regime and the rationale for each such action; and
- Communicating changes to the RFI's sanctions obligations, including changes to its sanctions-related policies, procedures and controls.

Documentation and record-keeping

6.47 RFIs should ensure that appropriate record is made of the following:

- The RFI's sanctions-related policies, procedures and controls;
- Actions taken to comply with the sanctions regime;
- Information sought and obtained to confirm or eliminate a potential match;
- The persons who decide whether a potential match is a true match; and
- The rationale for the decision.

6.48 All related records should be retained in accordance with the guidance provided in **Chapter 11: Record-Keeping**.

Reviewing effectiveness

6.49 Each RFI should monitor its policies, procedures and controls to ensure full, up-to-date and timely compliance with rapidly changing sanctions obligations.

6.50 An RFI should make the review of its sanctions-related policies, procedures and controls part of its AML/ATF independent audit. For additional information, see paragraphs 1.75 through 1.79.

6.51 Senior management is responsible for the effectiveness of an RFI's sanctions-related policies, procedures and controls. The Compliance Officer may be the appropriate person to grant authority to:

- Oversee the establishment, maintenance and effectiveness of the RFI's sanctions-related policies, procedures and controls;
- Monitor compliance with the relevant Acts, Regulations and guidance; and
- Access all necessary records in a timely manner in order to respond to any information gathering authorised by an Order.

Screening customers and transactions

6.52 RFIs should screen their business and transactions for any person, entity, activity or good that is a sanctions target. Screening should be conducted against appropriate lists, such as HM Treasury's Consolidated List of Targets and the lists of restricted goods linked at www.namlc.bm.

6.53 RFIs should screen not only their customers but wherever possible, any other related parties, including but not limited to, the following:

- Counterparties;
- Trustees and similar persons;
- Beneficial owners, directors, signatories and similar persons of customers, counterparties and third party service providers;
- Persons authorised by power of attorney; and
- The geographic connections of the abovementioned persons and entities.

6.54 At a minimum, each RFI should screen every related party for which verification of identity is sought under the RFI's risk-based policies, procedures and controls. For additional information, see **Chapter 4: Standard Customer Due Diligence Measures** and **Chapter 5: Non-Standard Customer Due Diligence Measures**.

6.55 Where an RFI chooses not to screen any customer or related party, the RFI should be aware that it is increasing its likelihood of committing a sanctions offence.

6.56 RFIs should screen the payment information associated with transfers of funds to identify any potential sanctions targets. RFIs should screen information contained within the payment messages, cover messages or batch files of any messaging system, as well as any information associated with the transfer of funds that is conveyed by any other means. An RFI may need to request additional information

in order to meet its sanctions obligations. For additional information, see paragraphs 8.23 through 8.63.

Timing and scope of screening

6.57 Initial screening of customers and related parties should take place during the establishment of a business relationship, or as soon as possible thereafter.

6.58 Where an RFI conducts screening after the establishment of a business relationship, it should be aware that it may transact with a sanctions target in breach of the sanctions. RFIs should consider conducting post-event screening only for incoming transactions, provided that the RFI maintains control over the funds or assets and no funds or assets are made available to any other parties prior to the completion of screening.

6.59 The screening of payment information should take place on a real-time basis. An RFI may accept an incoming payment prior to screening for a sanctions target, but it must not forward any payment, disburse any funds, or otherwise make funds or assets available to any party prior to screening.

Screening software

6.60 RFIs may choose to use commercially available screening software; other RFIs may rely on manual screening.

6.61 Where an RFI chooses to use screening software, the RFI should ensure that the software will flag potential matches with sanctions targets in a clear and prominent manner.

6.62 RFIs should understand the capabilities and limits of any software, and ensure that the software is appropriate given the nature and size of the business and the volume and types of data the business uses, including data held in any legacy systems.

6.63 Where automated software screening is used, RFIs should monitor and test the on-going effectiveness of the software, and ensure that adequate contingency arrangements are in place in the event that the software fails.

"Fuzzy matching"

6.64 RFIs should wherever possible use a screening system with "fuzzy matching" capabilities. "Fuzzy matching" describes any process that identifies non-exact matches. Where data in an RFI's records or in official sanctions lists is misspelled, incomplete or missing, a screening system with "fuzzy matching" capabilities will nonetheless identify potential matches. These capabilities are often tolerant of multinational and linguistic differences in spelling, transliteration, formats for dates of birth and similar data. "Fuzzy matching" systems may also screen for the reversal of names, the removal of numbers or the replacement of numbers with words, which are techniques that have been used in an attempt to evade sanctions.

6.65 A sophisticated "fuzzy matching" system will have a variety of settings, allowing RFIs to set greater or lesser levels of fuzziness in the matching process. In determining an appropriate level of fuzziness, an RFI should ensure that all potential matches are flagged and should calibrate its system with due regard to paragraph 7.18.

Reliance and outsourcing

6.66 The Acts and Regulations do not set forth any provision for reliance for the purposes of screening customers and transactions for sanctions compliance. In determining its screening policies, procedures and controls, an RFI should not assume that introduced business has been screened for sanctions compliance or that any screenings conducted were adequate or maintained up-to-date.

6.67 RFIs may choose to outsource to a third party service provider some or all of its sanctions screening or other sanctions-related processes, bearing in mind that an RFI cannot contract out of its statutory and regulatory obligations under the Bermuda sanctions regime. RFIs should ensure that the responsibilities in any outsourcing relationship are clearly set forth in a service level agreement and RFIs should satisfy themselves that the service provider is providing an effective service.

6.68 RFIs must not rely upon or enter into any outsourcing arrangement with a third party where access to data without delay is likely to be impeded by confidentiality, secrecy, privacy or data protection restrictions.

6.69 In contemplating any reliance or outsourcing relationship with a third party, RFIs should have due regard to paragraphs 5.118 through 5.178.

Reporting matches and breaches

6.70 RFIs should investigate potential matches with sanctions targets to determine whether there are any true matches.

6.71 A true match arises where an RFI knows or suspects that it is conducting or may conduct business involving a sanctions target. For additional information on the meaning of "knowledge" and "suspicion", see paragraphs 9.6 through 9.19.

6.72 In determining whether a potential match is a true match, an RFI should seek sufficient information from relevant parties to enable it to confirm or eliminate a potential match. An RFI should ensure that there is a clear rationale for any decision that a potential match is not a true match.

6.73 RFIs should maintain a record of the information sought and obtained, the person or persons involved in the review of the potential match, and the rationale for the decision made.

6.74 RFIs must ensure that they have clear internal and external reporting processes for reporting true matches to the Governor and the BMA. These reporting processes may involve the Reporting Officer and should be designed with due regard to the guidance provided in 9.22 through 9.49.

6.75 Where an RFI identifies a true match, it should verify whether the sanctions target is listed in an Order that has been given effect in Bermuda by virtue of its inclusion in Schedule 1 of the International Sanctions Regulations 2013.

<u>Where the sanction is in effect in Bermuda, the RFI must:</u>

- Immediately comply with the terms of the Order by freezing any funds or assets where required or taking any other required action; and
- Immediately inform the Governor in writing at:

The Governor of Bermuda

Government House
11 Langton Hill
Pembroke, HM13
Bermuda

Where the sanction is not effect in Bermuda, the RFI should:

- Immediately contact the Office of the NAMLC at:

  Office of the National Anti-Money Laundering Committee
  Ministry of Legal Affairs
  4th Floor, Global House
  43 Church Street
  Hamilton, HM12
  Bermuda

  Chairman: Ms. Cheryl-Ann Lister
  Telephone: 441 294-9797

  E-mail: info-namlc@gov.bm

in order to obtain advice on whether and how to proceed.

6.76 When informing the Governor of a true match, or that the RFI or a sanctions target has breached a sanction (see paragraph 6.25), an RFI should copy the BMA and include the following:

- The information or other matter on which the knowledge, suspicion or breach is based;
- Any information held by the RFI about the sanctions target by which the target can be identified; and
- The nature and amount, quantity or value of any funds or assets held by the RFI in relation to the sanctions target.

6.77 Where an RFI freezes assets, it should do so immediately upon discovering the true match and should ensure that relevant staff do not process any further transactions without an express direction from senior management.

6.78 Where a true match is identified before commencing a business relationship, an RFI should not accept the business unless it first applies for and obtains an appropriate license.

Licensing

6.79 An RFI may apply to the Governor for a license to release funds from a frozen account, make funds or assets available to, or for the benefit of, a sanctions target, or engage in any other activity that would otherwise be prohibited by a sanction.

6.80 If a license is granted, it will normally be accompanied by a letter stating the purpose of the license being issued and the precise scope of the activity the license authorises.

6.81 RFIs should ensure that appropriate policies, procedures and controls are in place to monitor whether any activity carried out in relation to a sanctions target is within the precise scope of any license obtained.

Suspicious activity reports

6.82 Holding an account for a sanctions target or processing a transaction which involves a sanctions target is not in itself grounds for filing a suspicious activity report with the FIA.

6.83 However, where an RFI has knowledge or suspicion that funds or assets are the proceeds of crime, or that a person is involved in ML/TF, the RFI must comply with its suspicious activity reporting obligations under the Acts and Regulations.

Customer notification and tipping-off

6.84 The fact that a target is subject to sanctions is public information and there is no prohibition on RFIs informing customers or third parties of a target's sanctioned status. Under POCA 1997 and ATFA 2004, informing customers or third parties of a target's sanctions status is not a tipping-off offence.

6.85 By contrast, where an RFI has filed a suspicious activity report with the FIA, disclosing the fact that the suspicious activity report was filed is a tipping-off offence.

CHAPTER 7 - ON-GOING MONITORING

Introduction

7.1 This chapter provides guidance for the requirement that RFIs conduct on-going monitoring of the business relationships with their customers.

7.2 The responsibilities of RFIs to conduct on-going monitoring are governed primarily by Regulations 7, 11(4)(c), 13(4), 16 and 18.

7.3 RFIs must conduct on-going monitoring of the business relationship with their customers.

7.4 On-going monitoring is an integral part of an RFI's AML/ATF program and supports several objectives:

- Maintaining a proper understanding of a customer's activities;
- Ensuring that CDD documents and other records are accurate and up to date;
- Providing accurate inputs for the RFI's risk assessment processes;
- Testing the outcomes of the RFI's risk assessment processes; and
- Detecting and scrutinising unusual or suspicious transactions.

7.5 Failure to adequately monitor a customer's business relationship could expose an RFI to abuse by criminals and may call into question the adequacy of the RFI's AML/ATF policies, procedures and controls, and the integrity or fitness and properness of the RFI's management.

7.6 On-going monitoring of a business relationship includes:

- Scrutinising transactions undertaken throughout the course of the relationship (including, where necessary, the source of wealth and/or source of funds) to ensure that the transactions are consistent with the RFI's knowledge of the customer and his risk profile;
- Investigating the background and purpose of all complex or unusually large transactions, and unusual patterns of transactions which have no apparent economic or lawful purpose, and recording in writing the findings of the investigation; and

- Reviewing existing documents, data and information to ensure that they are up-to-date, adequate and relevant for the purpose of applying CDD measures.

7.7 Guidance regarding the review of existing documents, data and information to ensure that they are up-to-date, adequate and relevant is provided in paragraph 3.21.

7.8 RFIs should determine the scope and frequency of on-going monitoring using a risk-based approach. RFIs should direct greater monitoring resources toward those products, services and business relationships presenting a higher risk of money laundering or terrorist financing than to those presenting a lower risk. RFIs must be able to demonstrate to their supervisory authority that the extent of their CDD measures and monitoring is appropriate in view of the risks of money laundering and terrorist financing.

7.9 In determining a proper allocation of monitoring resources, RFIs should consider:

- The size and complexity of the RFI;
- The nature, scope and delivery channels of the products and services the RFI provides;
- Any national risk assessment findings;
- The RFI's own risk assessment findings; and
- The nature, scope and effectiveness of the RFI's existing monitoring systems.

7.10 With respect to the customer, RFIs should consider:

- The nature, amount and frequency of the transactions;
- Geographic connections (see paragraph 2.48);
- Whether the customer is known to use other products and services;
- Whether the customer can be categorised according to activity or turnover and whether the customer's conduct falls outside any norms established for any categories identified; and
- Whether the customer presents a higher than standard risk for money laundering or terrorist financing.

Establishing norms

7.11 Bearing in mind that some criminal activity may be so widespread as to appear to be the norm, RFIs should establish norms for lawful transactions and conduct for its products or services, and for any categories of transaction or customer it designates. Once an RFI has established norms for lawful transactions and conduct, it must monitor the business relationship, including transactions and patterns of transactions, to identify transactions and conduct falling outside of the norm.

7.12 Where a relationship changes significantly, RFIs should apply further CDD measures to ensure a proper understanding of the relationship, including its purpose and nature, and to determine whether any transaction or conduct is unusual or suspicious.

7.13 RFIs should have policies, procedures and controls in place for customers who have not had contact with the RFI for some time, in circumstances where regular contact might be expected. Where an account or relationship is dormant, RFIs should be able to identify reactivation and any unauthorised use.

7.14 Depending on the nature of the business each RFI carries out, and the nature of its customer portfolio, each RFI should establish norms for cash transactions and the identification of unusual cash transactions or proposed cash transactions. Given the international nature of business conducted by many RFIs, cash transactions may be relatively uncommon, whereas for many banks, building societies or money services businesses offering services to local customers, cash transactions may be a normal every-day service.

Systems for monitoring

7.15 Monitoring may take place both in real time as transactions or conduct take place and after the event by reviewing the transactions or conduct that a customer has undertaken. Irrespective, any system of monitoring should ensure at its core that:

- Transactions and conduct are flagged in exception reports for further examination;
- The exception reports are reviewed promptly by the appropriate person(s); and
- Appropriate and proportionate action is taken to reduce the possibility of money laundering or terrorist financing occurring without detection.

7.16 An RFI should calibrate its monitoring systems to identity for review all higher-risk activity, including:

- All complex or unusually large transactions and unusual patterns of transactions which have no apparent economic or lawful purpose;
- Transactions or conduct falling outside of the expected norm for a customer, product or service; and
- Transactions or conduct involving the circumstances described in paragraphs 5.17 through 5.18.

7.17 ML/TF typologies are numerous and constantly evolving. The employees involved in the design, application and updating of a monitoring system should understand the range of potential indicators of suspicious transactions, and conduct as they pertain to the RFI's products, services and delivery channels. An RFI's monitoring system should apply the full range of potential indicators to the transactions and conduct being monitored.

7.18 An RFI should not calibrate its monitoring system to produce only the volume of transaction reporting that existing employees are capable of reviewing. Therefore, the RFI should determine if additional compliance resources are necessary to monitor and review the risks present in its business. Likewise, an RFI should calibrate its monitoring system to avoid producing large numbers of 'false positives', which require excessive employee resources to scrutinise.

Automated monitoring

7.19 Subject to the needs identified through an RFI's risk analysis, a monitoring system may be either manual or automated to the extent that a standard suite of exception reports is produced. Larger RFIs and RFIs with greater volume or turnover associated with a particular product or service are more likely to require some level of automated monitoring.

7.20 Where an automated or computerised system is contemplated, RFIs should satisfy themselves that:

- The system sufficiently monitors for appropriate money laundering and terrorism typologies;
- The typologies for which the system monitors are regularly updated;

- The system is appropriate for and/or sufficiently adjustable to the product or service to which it is to be applied;
- The system provides the user with the reasons that unusual customer behaviour or a transaction is flagged; and
- The system is capable of calibration in accordance with paragraph 7.18.

7.21 Where an automated monitoring system is used, RFIs should ensure that staffing levels and skill sets are appropriate for the purpose of overseeing the automated system. Certain tasks and skills cannot be automated, including employee intuition, perceptions acquired through direct interaction with a customer and the ability, through practical experience, to recognise transactions that appear to fall outside of the established norm for a product, service or customer.

CHAPTER 8 - WIRE TRANSFERS

Introduction

8.1 This chapter provides guidance on appropriate policies, procedures and controls to ensure that all transfers of funds can be effectively traced to the parties involved in the transaction.

8.2 The transfer of funds requirements for RFIs is governed primarily by Regulations 21 through 31. Penalties specific to violations of the abovementioned Regulations are set forth in Regulation 32.

8.3 Regulations 21 through 32 are directed toward enhancing the transparency of all transfers of funds, both cross-border and domestic. Specifically, the Regulations require RFIs to ensure that essential information on both the payer and payee of each transfer is accurate, complete and immediately available to the following entities:

- RFIs providing transfer services as a payer RFI, intermediary RFI or payee RFI, to facilitate the identification and reporting of suspicious transactions; and
- Competent authorities, to assist them in tracing the transactions of money launderers, terrorists and other criminals for the purposes of investigation and prosecution.

Scope of the Regulations

8.4 Any RFI that provides services for the transfer of funds, whether as a payer RFI, intermediary RFI or payee RFI, is a PSP bound by the regulations governing wire transfers.

8.5 The Regulations cover all types of transfers in any currency whether domestic or cross-border, carried out by or on behalf of a payer through a PSP by electronic means in order to make funds available to a payee at a PSP, irrespective of whether an intermediary PSP is involved, irrespective of whether the payer and the payee hold accounts with the same PSP, and irrespective of whether the payer and the payee are the same person.

8.6 For Bermuda-based PSPs the Regulations cover international transfers and domestic transfers.

8.7 Despite the broad application of the Regulations, several transfer types are exempted in part or in whole from the Regulations. Regulation 22 grants specified exemptions for the following:

- Transfers where both the payer and payee are PSPs acting on their own behalf, and not on behalf of any underlying customer. This exemption applies to MT 200 series payments via SWIFT and includes MT 400 and MT 700 series messages when they are used to settle trade finance obligations between banks;

- Transfers by credit or debit card or similar payment instrument, provided that the payee has an agreement with the PSP permitting payment for goods or services and that the transfer is accompanied by a unique identifier permitting the transaction to be traced back to the payer (for more information, see paragraph 8.32);

- Transfers whereby the payer withdraws cash from his or her own account. This is designed to exempt ATM withdrawals outside Bermuda that would otherwise require complete information to be included with the transfer;

- Transfers to public authorities within Bermuda for taxes, fines or other levies;

- Direct debits, provided they carry a unique identifier for tracing purposes;

- Truncated cheques (cheques are otherwise paper to which the Regulation does not apply);

- Pre-paid transfers in amounts not exceeding $150 that are carried out by means of a mobile phone or any other digital or IT device; and

- Post-paid transfers carried out by mobile phone or any other digital or IT device, provided that the transfer relates to the provision of goods and services, a unique identifier accompanies the transfer and the payee's PSP is AML/ATF regulated financial institution in Bermuda or in a jurisdiction that imposes equivalent AML/ATF requirements.

Complete information

8.8 PSPs must ensure that transfers of funds are accompanied by complete information on both the payer and payee.

8.9 Complete information on the payer means:

- The payer's name;
- The payer's address; and
- The payer's account number.

8.10 Complete information on the payee means:

- The payee's name; and
- The payee's account number.

8.11 Where the payer is a private individual, the payer's address may be substituted with the payer's date and place of birth, customer identification number or national identity number. PSPs should allow this substitution only to address legitimate business needs, and should use the substitution only in limited circumstances where the risks associated with a departure from the standard are objectively justified and documented. As a general practice, each PSP should ensure that its terms and conditions of business with each payer address the release of the complete information described in paragraphs 8.9 through 8.17 to other PSPs involved in the execution of the transfer.

8.12 Where the payer is a legal person, the address should be the address where the company's business is conducted.

8.13 Where the payer is a trust or trustee, the address should be the address of the trustee.

8.14 Where a payer is a bank acting on its own behalf and not on behalf of any underlying customer, the Bank Identifier Code (BIC) constitutes complete payer information. Nonetheless, the account number should be included where available. Where a payer has a Business Entity Identifier (BEI) or Legal Entity Identifier (LEI), the BEI or LEI, together with the account number, constitute complete payer information. Institutions utilising BICs, BEIs or LEIs should be

aware that the omission of an address may result in requests for the address from an intermediary PSP or payee PSP.

8.15 Where the payer does not have an account number, the account number may be substituted with a unique identifier that allows the transaction to be traced back to the payer. See paragraph 8.32.

8.16 Account numbers may be, but are not required to be, expressed in IBAN (International Bank Account Number) format.

8.17 Although it is possible that a payee may in fact be a conduit for an undisclosed "final recipient" to serve a criminal objective, PSPs should understand the payee to be the person named in the transfer as the beneficiary of the payment unless there is evidence to suggest that another person will benefit.

Cross-border transfers of funds

8.18 A transfer of funds is a cross-border transfer if any payer PSP, intermediary PSP or payee PSP involved in executing the transfer is located outside of Bermuda.

8.19 Where any portion of a transfer is cross-border, PSPs should treat all aspects of the transfer as being cross-border.

8.20 Due to the nature of the financial industry in Bermuda, the vast majority of transfers with which Bermudian PSPs are involved are cross-border.

8.21 A Bermudian PSP should transact only with non-Bermudian PSPs that it has approved using an appropriate risk-assessment. Bermudian PSPs should ensure that any non-Bermudian PSP implements the wire transfer standards set forth by the Financial Action Task Force.

8.22 Before a Bermudian PSP enters into or elects to maintain a correspondent banking relationship with any non-Bermudian PSP, the Bermudian PSP should ensure that it understands and has vetted the beneficial ownership of any non-Bermudian PSP that is not listed on an appointed stock exchange and subject to Bermuda disclosure obligations or to disclosure obligations equivalent to those in Bermuda.

Obligations on payer PSPs

8.23 Payer PSPs must ensure that each cross-border transfer of funds includes complete information on the payer and payee.

8.24 Where the payer is an accountholder at the Payer PSP, the Payer PSP must ensure, before transferring funds, the complete information on the payer conveyed in the payment is accurate and has been verified.

8.25 The complete information of an account-holding payer is accurate and verified if the information has been satisfactorily obtained and verified, in accordance with the Regulations and these Guidance Notes. However, a number of factors may cause a PSP to conduct additional customer due diligence on an accountholder prior to authorising the transfer. These factors include but are not limited to the PSP's risk tolerance and risk assessments, the involvement of any third party service provider, the involvement of higher-risk persons or jurisdictions and the particular nature of the transfer that has been requested, in the context of the accountholder's previous transactions and conduct.

8.26 The extent of the information supplied in each field of the payment message is subject to the conventions of the messaging system in question.

8.27 In the case of a transfer from a joint account, a PSP may demonstrate that it has met its legal obligation to provide a customer name where, dependent on the size of the field, it provides the name of either or both account holders.

8.28 PSPs should send payments through a messaging system capable of carrying all of the complete information on the payer and payee. Where the size or types of a messaging system's fields are such that the complete information cannot be included, the PSP should use a different messaging system or provide the complete information to the payee PSP and any intermediary PSPs by an agreed form of communication, whether within a messaging system or otherwise.

8.29 The payer's name, address (or permitted alternative) and account number should match the information that the PSP holds in respect of the payer's account(s). PSPs generally populate the messaging system's information fields from customer

databases. Any request to alter the customer information sent via the messaging system should be subject to a rigorous and documented referral and approval mechanism. This is to ensure that the transfer instruction is approved on an exceptional basis only in cases where the PSP is entirely satisfied that the reason for quoting alternative information with a payer's account number is legitimate.

8.30 Where the payer is not an accountholder and the transfer exceeds $1,000, the payer PSP must satisfactorily obtain, and verify the identity and address of the payer prior to executing the transaction. Where the address is substituted with a payer's date and place of birth, customer identification number or national identity number, that information must also be verified. In addition, PSPs must verify the complete information where a transaction is carried out in several operations that appear to be linked and together exceed $1,000.

8.31 Where the payer is not an accountholder and the transfer is $1,000 or less, the payer PSP must obtain information establishing the payer's identity and address. Where the address is substituted with a payer's date and place of birth, customer identification number or national identity number, that customer information must be obtained. PSPs are not required to verify the information obtained for such transactions; nonetheless, it is advisable to do so in all cases. Where a transaction is carried out in several operations that appear to be linked and together exceed $1,000, the verification requirements described in paragraph 8.30 apply.

8.32 Where the payer is not an accountholder or the transfer is otherwise not drawn from a bank account, the payer PSP must produce and include with the transfer a unique identifier that allows that allows the transaction to be traced back to the payer. The Regulations distinguish between a "unique identifier" and a "customer identification number". The unique identifier identifies a payment and allows it to be traced back to a payer. The customer identification number identifies a payer and refers to a record held by the payer PSP that contains a customer's name and address, national identity number, or date and place of birth.

8.33 For all transfers of funds, where all of the required information is not available or where any of the information that is available is meaningless or otherwise incomplete, payer PSPs should not allow the transfer to be executed. In practice, some messaging systems will allow a transfer to proceed without each required field being populated. PSPs should nonetheless have risk-based policies,

procedures and controls to identify and prevent transfers for which meaningless or incomplete information has been included in any field.

8.34 Payer PSPs should consider all aspects of ordering and executing a transfer as factors in assessing whether the transfer of funds, or any related transaction, is suspicious and whether a report must be made to the Reporting Officer. Circumstances that may indicate a transfer of funds, or any related transaction, is suspicious include, but are not limited to:

- A payer who is unwilling or unable to provide the complete information required;
- A payer for whom the complete information cannot be verified, where it is required to do so;
- A payer seeking to alter the customer information sent via the messaging system, for reasons that the PSP is not able to fully confirm as legitimate;
- A transfer with missing, meaningless or otherwise incomplete information;
- A payer seeking to route the transaction through apparently unnecessary intermediary PSPs; and
- A payer seeking to ensure that the complete information does not reach all PSPs involved in the execution of the payment.

8.35 The payer PSP should maintain records of all information received from the payer. The payer PSP should also maintain records of all information received from the payee PSP and any intermediary PSPs, including requests for information. All records should be kept in accordance with the guidance provided in **Chapter 11: Record-Keeping**.

Obligations on intermediary PSPs

8.36 Intermediary PSPs must ensure that, for each cross-border transfer of funds, all information received on the payer and payee is kept with the transfer.

8.37 Intermediary PSPs should forward transfers through a messaging system capable of carrying all of the complete information on the payer and payee.

8.38 Where technical limitations associated with a messaging system prevent all information received on the payer and payee from accompanying the transfer, an

intermediary PSP may nonetheless use the messaging system with technical limitations, provided that:

- The intermediary PSP forwards all of the complete information on the payer and payee; and
- The intermediary PSP is not aware that any of the complete information on the payer or payee is missing, meaningless or otherwise incomplete.

8.39 Where the intermediary PSP is aware that any of the complete information on the payer or payee is missing, meaningless or otherwise incomplete, it may nonetheless use a messaging system with technical limitations provided that:

- The intermediary PSP informs the payee PSP and any downstream intermediary PSPs of the missing, meaningless or otherwise incomplete information by an agreed form of communication, whether within a messaging service or otherwise;
- The intermediary PSP retains record of all information received on the payer and payee for five years; and
- The intermediary PSP provides the payee PSP with all information received on the payer and payee within three working days of receiving any request by the payee PSP.

8.40 Intermediary PSPs should have risk-based policies, procedures and controls for the following:

- Identifying transfers, including those carried out with straight-through processing, that are lacking any required information;
- Determining when to execute, reject or suspend such transfers; and
- Determining appropriate follow-up action with payer PSPs, payee PSPs, any other intermediary PSPs and competent authorities.

8.41 Where an intermediary PSP knows or suspects that information provided by the payer PSP has been stripped or altered at any point in the payment chain, it should:

- Reject the transfer;
- Request the complete information on the payer and payee; or
- Make an internal suspicious activity report to the Reporting Officer.

8.42 At all times, PSPs must adhere to the Acts, Regulations and Guidance Notes addressing tipping-off offenses. For more information, see paragraphs 9.80 to 9.86.

8.43 Intermediary PSPs should consider all aspects of receiving and forwarding a transfer of funds as factors in assessing whether the transfer of funds, or any related transaction, is suspicious and whether a report must be made to the Reporting Officer. Circumstances that may indicate a transfer of funds or any related transaction is suspicious include but are not limited to:

- A transfer with missing, meaningless or otherwise incomplete information;
- A transfer that has been routed through one or more intermediary PSPs, apparently without a legitimate purpose; and
- A transfer that appears to have been routed through the intermediary PSP for the purpose of preventing information from reaching the payee PSP.

8.44 The intermediary PSP should maintain records of all information received from the payer PSP, payee PSP and any other intermediary PSPs. All information includes information that pertains to the payment, including requests for information, whether received through a messaging system, or through any other means. All records should be kept in accordance with the guidance provided in **Chapter 11: Record-Keeping**.

Obligations on payee PSPs

8.45 Payee PSPs should ensure that the identity of the payee is accurate and verified for any cross-border transfer of funds over $1,000, and for any cross-border transaction that is carried out in several operations that appear to be linked and together exceed $1,000.

8.46 Where the payee is an accountholder at the Payee PSP, the payee's identity is accurate and verified, if the information has been satisfactorily obtained and verified in accordance with the Regulations and these Guidance Notes. However, a number of factors may cause a PSP to conduct additional customer due diligence on an accountholder prior to disbursing any funds from the transfer. These factors include but are not limited to the PSP's risk tolerance and risk assessments, the involvement of any third party service provider, the involvement

of higher-risk persons or jurisdictions, and the particular nature of the transfer that has been received in the context of the accountholder's previous transactions and conduct.

8.47 Where the payee is not an accountholder and the transfer exceeds $1,000, the payee PSP should satisfactorily obtain and verify the identity of the payee prior to the disbursement of any funds to the payee. In addition, PSPs must verify the identity of the payee where a transaction is carried out in several operations that appear to be linked and together exceed $1,000.

8.48 Where the payee is not an accountholder and the transfer is $1,000 or less, the payee PSP should obtain information establishing the payer's identity. PSPs are not required to verify the information obtained for such transactions; nonetheless, it is advisable to do so in all cases. Where a transaction is carried out in several operations that appear to be linked and together exceed $1,000, the verification requirements described in paragraph 8.47 apply.

8.49 Where the payee is not an accountholder, the payee PSP should ensure that the payer PSP produced and included with the transfer a unique identifier that allows the payment to be traced back to the payer. For more information, see paragraph 8.32.

8.50 Payee PSPs must have effective procedures to detect whether incoming transfers of funds include all required information.

8.51 In practice, some messaging systems will not allow a transfer to reach a payee PSP without each required field being populated. Payee PSPs should nonetheless have risk-based policies, procedures and controls to identify transfers for which meaningless or incomplete information has been included in any field.

8.52 Where feasible, monitoring for missing, meaningless or otherwise incomplete information should be carried out in real time and prior to the disbursement of any funds to a payee.

8.53 Where a payee PSP becomes aware in the course of processing a payment that it is missing required information, or that the required information provided is meaningless or otherwise incomplete, the payee PSP must:

- Reject the transfer;
- Request the complete information on the payer and payee; or
- Make an internal suspicious activity report to the Reporting Officer.

8.54 A payee PSP should also take one or more of the steps outlined in paragraph 8.53 where it knows or suspects that information provided by the payer PSP has been stripped or altered at any point in the payment chain.

8.55 At all times, PSPs must adhere to the Acts, Regulations and Guidance Notes addressing tipping-off offenses. For more information, see paragraphs 9.80 through 9.86.

8.56 Where a payer PSP regularly fails to provide all required information on the payer and payee, the payee PSP must inform the BMA and take steps to ensure that the payer PSP provides all required information. Steps a payee PSP may take in such a situation include but are not limited to issuing warnings to the payer PSP and setting deadlines for the payer PSP to provide all required information.

8.57 Where, despite the payee PSP taking the steps described in paragraph 8.56, a payer PSP still regularly fails to provide all required information on the payer and payee, the payee PSP should terminate its business relationship with the payer PSP, either completely or in respect of funds transfers.

8.58 Payee PSPs should also apply paragraphs 8.56 through 8.57 to intermediary PSPs that regularly fail to provide the complete information on the payer and payee, or that regularly fail to provide upon request all information received on the payer and payee from the payer PSPs and any other intermediary PSPs.

8.59 Where real time monitoring is not feasible, payee PSPs should conduct post-event monitoring through the use of risk-based sampling. Such sampling may include but is not limited to:

- Cross-border transfers of funds as defined in paragraph 8.18;
- Transfers involving higher-risk customers and jurisdictions, as identified by the PSP's business risk assessment and reliable external sources;
- Transfers involving multiple intermediaries;
- Transfers involving payer PSPs or intermediary PSPs that have previously failed to provide all required information;

- Transfers involving PSPs known via reliable sources to have stripped or altered information provided by the payer PSP;
- Transfers for which alternative information has been substituted for the payer's address;
- Transfers above the $1,000 threshold to non-accountholders; and
- Transfer chains involving two or more PSPs that are bound by different sanctions regimes.

8.60 Payee PSPs must consider all aspects of receiving a transfer of funds as factors in assessing whether the transfer of funds, or any related transaction, is suspicious and whether a report must be made to the Reporting Officer. Circumstances that may indicate a transfer of funds or any related transaction is suspicious include but are not limited to:

- A transfer with missing, meaningless or otherwise incomplete information;
- A transfer that has been routed through one or more intermediary PSPs, apparently without a legitimate purpose;
- A transfer that appears to have been routed through one or more intermediary PSPs for the purpose of preventing information from reaching the payee PSP; and
- A transfer for which there is evidence to suggest that a person other than the named payee is the intended final recipient.

8.61 Although it is possible that a payee may in fact be a conduit for an undisclosed "final recipient" to serve a criminal objective, PSPs should understand the payee to be the person named in the transfer as the beneficiary of the payment, unless there is evidence to suggest that another person will benefit.

8.62 The payee PSP must maintain records of all information received from the payer PSP and any intermediary PSPs. All information includes information that pertains to the transfer, whether received through a messaging system or through any other means. The payee PSP must also maintain records of its verifications of payee identities. All records should be kept in accordance with the guidance provided in **Chapter 11: Record-Keeping**.

Batch file transfers

8.63 Under Regulation 25, the batch file for transfers from a single payer to multiple payees outside Bermuda must contain complete information on the payer and payee. However, the individual transfers within the batch need carry only the following:

- The account number of the payer (or where an account number is not available, a unique identifier);
- The account number of the payee (or where an account number is not available, a unique identifier); and
- The payee's name.

Domestic transfers of funds

8.64 Where the payer PSP, payee PSP and any and all intermediary PSPs are all located within Bermuda, transfers of funds need be accompanied only by the payer's account number or by a unique identifier which permits the transaction to be traced back to the payer.

8.65 The payer PSP must provide the payee PSP with the complete information on the payer within three working days of receiving any request from the payee PSP.

Money or value transfer service providers

8.66 Money or value transfer service providers are required to comply with the Acts, Regulations and Guidance Notes addressing wire transfers.

8.67 Where a money or value transfer service provider controls both the payer PSP and payee PSP, the service provider should:

- Consider all information from both the payer PSP and payee PSP in determining whether an external suspicious activity report must be filed; and
- File any external suspicious activity report in each jurisdiction affected by the suspicious transfer and make the transaction information available to each jurisdiction's financial intelligence unit which in the case of Bermuda is the Financial Intelligence Agency.

Minimum standards

8.68 The above information requirements are minimum standards. It is open to PSPs to elect to supply the complete information on the payer and payee with transfers that are eligible for a reduced information requirement. Doing so limits the likely incidence of inbound requests for the complete information.

8.69 It is also open to PSPs to request the complete information from payer PSPs and intermediary PSPs in order to ascertain the degree to which accurate and complete information travels through particular PSPs.

CHAPTER 9 - SUSPICIOUS ACTIVITY REPORTING

Introduction

9.1 This chapter provides guidance on the suspicious activity reporting procedures appropriate for an RFI to meet its obligations under Bermuda's AML/ATF Acts and Regulations.

9.2 The suspicious activity reporting requirements for RFIs are governed primarily by Sections 43 through 48 of POCA 1997, Sections 5 through 12 of ATFA 2004, and Regulations 16 and 17.

9.3 RFIs must put in place appropriate policies and procedures to ensure that knowledge or suspicion that funds or assets are the proceeds of crime or that a person is involved in money laundering or terrorist financing are identified, enquired into, documented and reported.

9.4 An RFI's policies and procedures for suspicious activity reporting must ensure that:

- The RFI's employees are trained to identify and report suspicious activity related to proceeds of crime, ML/TF;
- The RFI's employees provide an internal report to the Reporting Officer where there is knowledge, or suspicion that funds or assets are the proceeds of crime, or that a person is involved in money laundering or terrorist financing;
- The RFI's Reporting Officer considers all internal reports in light of all relevant and available information, and requires appropriate enquiries to be made;
- The RFI's Reporting Officer makes external reports to the Financial Intelligence Agency as soon as is practicable where the Reporting Officer finds that that the report, in light of all relevant and available information, evidences knowledge or suspicion that funds or assets are the proceeds of crime, or that a person is involved in money laundering or terrorist financing;
- The RFI does not make any funds available to any person specified by written notice received from the Financial Intelligence Agency for a period not exceeding 72 hours; and
- The RFI's employees understand that it is a criminal offence to disclose to any person other than the Reporting Officer or the Financial Intelligence Agency,

any knowledge or suspicion that a disclosure has been filed with the Financial Intelligence Agency, or any other information or other matter likely to prejudice any investigation, which might be conducted following such a disclosure.

9.5 Sole traders that neither employ nor act in association with any other person are not required to put in place policies and procedures to ensure that suspicious activity is reported. They must nonetheless make an external report to the Financial Intelligence Agency as soon as is reasonably practicable where there is knowledge or suspicion that funds or assets are the proceeds of crime, or that a person is involved in money laundering or terrorist financing.

What is meant by "knowledge" and "suspicion"?

Knowledge

9.6 Having knowledge means knowing the existence of certain facts. In a criminal court, to have knowledge, it must be proved that the individual in fact knew that funds or assets were the proceeds of crime, or that a person was engaged in money laundering or terrorist financing.

9.7 However, knowledge can be inferred from the surrounding circumstances. A failure to ask the questions that an honest and reasonable person in similar circumstances would have asked may be relied upon by a jury to imply knowledge.

9.8 Section 46 of POCA 1997 and Schedule 1 of ATFA 2004 address knowledge that comes to a person in the course of their trade, profession, business or employment. Although information that comes to persons in other circumstances does not come within the scope of those Acts, persons may nonetheless choose to report such information.

Suspicion

9.9 Suspicion is subjective. Suspicion must be more than a vague feeling of unease; it may not be self-induced. At the same time, suspicion does not need to be clear or firmly grounded. Suspicion is sufficiently established when a relevant employee thinks "I have a suspicion but I cannot prove it by fact or hard evidence."

9.10 LEFT BLANK INTENTIONALLY

9.11 LEFT BLANK INTENTIONALLY

9.12 Guidance regarding the establishment of norms for transactions or activities, and the identification of unusual transactions or activities that fall outside of those established norms, is provided in paragraphs 7.11 through 7.14.

9.13 A transaction or activity that appears unusual is not necessarily suspicious. Even customers with a stable and predictable transactions profile will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. A transaction or activity that is identified as unusual, therefore, should not be automatically considered suspicious but should cause the RFI to conduct further, objective enquiries to determine whether or not the transaction or conduct is indeed suspicious.

9.14 Enquiries into unusual transactions should be in the form of additional CDD measures to ensure an adequate, gap-free understanding of the relationship, including the purpose and nature of the transaction and/or conduct in question.

9.15 Any approach to the customer or to an introducing intermediary should be made with due regard to the risk of violating the tipping-off rules of Section 47 of POCA 1997 and Section 10A of ATFA 2004. For further guidance, see paragraphs 9.83 through 9.84.

9.16 Where an employee conducts enquiries regarding an unusual transaction or conduct and obtains what a reasonable person in similar circumstances would consider to be a satisfactory explanation of the transaction or conduct, he may conclude that there are no grounds for suspicion and he may conclude the enquiries by making a record of his findings. However, where the employee's enquiries do not provide a satisfactory explanation of the transaction or conduct, he must conclude that there are grounds for suspicion and must make an internal report.

9.17 A report of each enquiry made in respect of an unusual transaction or activity should be documented or recorded electronically and retained in accordance with the guidance provided in **Chapter 11**.

9.18 A transaction or activity may not be suspicious at the time it takes place but suspicions that arise at a later time must nonetheless be reported. Where an intended transaction or activity appears suspicious (whether or not it ultimately took place), an internal report should be made before the suspicious transaction or conduct occurs. Where a transaction or activity appears suspicious only in hindsight, an internal report must be made after the transaction or activity has been completed.

9.19 Internal reports that are made after the transaction or activity has taken place are not intended as alternatives to reports that should have been made prior to the completion of the transaction or activity.

Non-Bermuda offences

9.20 Under Section 45(b) of POCA 1997, the offence of money laundering and the duty to report apply in relation to the proceeds of any criminal conduct, wherever carried out, that would constitute an offence if it took place in Bermuda. This broad scope excludes only those offences which the RFI, employee or Reporting Officer knows or believes to have been committed in a country or territory other than Bermuda and to be lawful under the law then applying in the country or territory concerned.

9.21 Under Section 17 of ATFA 2004, the duty to report applies in relation to any terrorist financing offence under Sections 5 through 8 of that Act which would have been an offence under these sections of the Act had it occurred in Bermuda.

Internal suspicious activity reporting

9.22 All employees, regardless of whether they have a compliance function, are obliged to report to the Reporting Officer within the RFI each instance in which they have knowledge or suspicion that funds or assets are the proceeds of crime or that a person is involved in money laundering or terrorist financing.

9.23 Internal suspicious activity reports to the Reporting Officer must be made as soon as is reasonably practicable.

9.24 RFIs must establish internal reporting procedures that, among other things, ensure that all employees know when, how and to whom they must report.

9.25 All internal reports of knowledge or suspicion must reach the Reporting Officer.

9.26 Line managers may be permitted to add comments to an internal report indicating evidence that may assist the Reporting Officer in determining whether the suspicion is justified but no line manager or any other person may prevent an internal report from reaching the Reporting Officer.

9.27 Whether or not an employee consults a colleague, the legal obligation remains with the employee to decide independently whether a report should be made; he must not allow any colleague to decide for him.

9.28 Reporting lines should be short with a minimum number of people between the person with reason to report and the Reporting Officer. Such an approach ensures speed, confidentiality and integrity in the reporting process, and swift access to the Reporting Officer.

9.29 Each internal report to the Reporting Officer should be documented or recorded electronically and retained in accordance with the guidance provided in **Chapter 11**.

9.30 Each internal report should include full details of the customer or transaction in question and as full a statement as possible of the information or activity giving rise to the knowledge or suspicion .

9.31 Where a Bermuda RFI is performing outsourcing functions for an institution outside of Bermuda and an external suspicious activity report is to be filed outside of Bermuda, the Bermuda RFI must also submit an external suspicious activity report to the Bermuda Financial Intelligence Agency. See paragraphs 9.49 and 9.85.

9.32 If during the processing of an application to open an account, during the establishment of a legal person or during the provision of a service to an existing

customer, an employee of a Bermuda RFI performing outsourcing functions has knowledge or suspicion, an internal report must be made to the Bermuda RFI's Reporting Officer.

9.33 Once an employee has reported his suspicion in an appropriate manner to the Reporting Officer or to an individual to whom the Reporting Officer has delegated the responsibility to receive such internal reports, he has fully satisfied his statutory obligation.

9.34 Unless the Reporting Officer advises the employee making an internal report to the contrary, further transactions or activities in respect of that customer or account, whether of the same nature or different from that giving rise to the previous suspicion, should be reported to the Reporting Officer as they arise.

Evaluation and determination by the Reporting Officer

9.35 The Reporting Officer must have the ultimate authority to evaluate internal suspicious activity reports and to determine whether an external suspicious activity report is appropriate under the Acts and Regulations.

9.36 An RFI's Reporting Officer must consider each report in light of all available information and determine whether it gives rise to knowledge or suspicion that funds or assets are the proceeds of crime or that a person is involved in money laundering or terrorist financing.

9.37 The Reporting Officer must diligently consider all relevant material to ensure that no vital information is overlooked when determining whether to make an external report to the Financial Intelligence Agency.

9.38 The RFI must permit the Reporting Officer to have access to its personnel and any relevant information, including CDD information, in the RFI's possession. The Reporting Officer must also have the ability to require additional relevant information to be obtained from the customer if necessary or from any relied upon party or any party carrying out AML/ATF measures under an outsourcing arrangement. See paragraphs 5.134 through 5.138 and 5.167 through 5.168.

9.39 Additional relevant information may include that which arises:

- Commercially, through linked accounts, third party service providers and introducers;
- Individually, through persons such as third parties, beneficial owners, controllers or signatories; or
- Through other means, including publically available information.

9.40 Any approach to the customer or to a relied upon party or introducing intermediary should be made with due regard to the risk of violating the tipping-off rules of Section 47 of POCA 1997 and Section 10A of ATFA 2004. For further guidance, see paragraphs 9.83 through 9.84.

9.41 When evaluating an internal report, the Reporting Officer taking account of the risk posed by the transaction or activity in question should strike the appropriate balance between the requirement to make a timely disclosure to the Financial Intelligence Agency and any delays that might arise in seeking additional relevant information.

9.42 Given the need for timely reporting, the Reporting Officer should consider when it is appropriate to make an initial report to the Financial Intelligence Agency prior to completing a full review of the business relationship and any linked or connected relationships. Any initial report must be followed by a full suspicious activity report as soon as is reasonably practicable. For additional information, see paragraph 9.52.

9.43 If the Reporting Officer determines that a report to the Financial Intelligence Agency is not appropriate, the reasons for the determination should be clearly documented or recorded electronically and retained in accordance with the guidance provided in **Chapter 11**.

External suspicious activity reporting

9.44 Where, after evaluating an internal suspicious activity report, the Reporting Officer determines that there is knowledge or suspicion that funds or assets are the proceeds of crime or that a person is involved in money laundering or terrorist financing, the Reporting Officer must file an external suspicious activity report with the Financial Intelligence Agency.

9.45 RFIs should include in each external report as much relevant information about the customer, transaction, counterparty or activity as it has in its records.

9.46 Each external report must be made as soon as is reasonably practicable after the information comes to the attention of the Reporting Officer.

9.47 Each external report to the Financial Intelligence Agency should be documented or recorded electronically and retained in accordance with the guidance provided in **Chapter 11**.

9.48 For all AML/ATF matters, contact between particular departments or branches of an RFI and the Financial Intelligence Agency or law enforcement should be controlled through or reported back to a single contact point, which is the Reporting Officer. Where matters do not relate to AML/ATF matters, it may be appropriate to route communications through an appropriate employee in the RFI's legal or compliance department.

9.49 Within a financial sector group, where a Bermuda RFI's internal suspicious activity report to a non-Bermuda parent or head office results in an external report to a non-Bermuda authority, the Bermuda RFI must also make an external report to the Financial Intelligence Agency.

Where to report

9.50 To avoid committing a failure to report offence, Reporting Officers must make their external reports to the Financial Intelligence Agency the central point for reporting of suspicions and, where appropriate, for providing consent to proceed with the transaction or activity.

9.51 As of October 2011, the Financial Intelligence Agency no longer accepts any manually submitted suspicious activity reports (including those faxed or emailed). The Financial Intelligence Agency accepts only those suspicious activity reports that are submitted electronically via the goAML system, which is available at **www.fia.bm**

9.52 Where a Reporting Officer has concluded that an external report should be made urgently, initial notification to the Financial Intelligence Agency may be made by

telephone but must be followed up by a full suspicious activity report as soon as is reasonably practicable.

9.53 The Financial Intelligence Agency is located at 6th Floor, Strata 'G' Building, 30A Church Street, Hamilton HM11 and it can be contacted during office hours on telephone number (441) 292-3422, on fax number (441) 296-3422 or by email at info@fia.bm

Disclosure of knowledge or suspicion of money laundering

9.54 Section 46 of POCA 1997 and Schedule 1 of ATFA 2004 require RFIs to report:

- Knowledge or suspicion that currency, funds or other assets are derived from or used in connection with any criminal conduct; and
- Knowledge or suspicion that a ML/TF offence has been committed, is in the course of being committed or has been attempted.

9.55 Such reports should be made regardless of whether the attempted activity actually occurs.

Penalties

9.56 Where an employee fails to comply with the obligations under Section 46 of POCA 1997 or Schedule 1 of ATFA 2004 to make disclosures to a Reporting Officer and/or to the Financial Intelligence Agency as soon as is reasonably practicable after information giving rise to knowledge or suspicion comes to the attention of the employee, the employee is liable to criminal prosecution.

9.57 The criminal sanction, under POCA 1997 and ATFA 2004, for failure to report is a prison term of up to three years on summary conviction or ten years on conviction on indictment, a fine up to an unlimited amount, or both.

Financial Intelligence Agency response and consent

9.58 External reports to the Financial Intelligence Agency that are made through the goAML system will be immediately acknowledged.

9.59 Under Article 15 of the Financial Intelligence Agency Act 2007, the Financial Intelligence Agency may serve a notice on an RFI in Bermuda requiring it not to

make available any funds to any person specified in the notice. RFIs must freeze the funds in any such order for a period not exceeding 72 hours.

Consent

9.60 Where an RFI files an external report and wishes to proceed with the suspicious transaction or activity, it should first request the express consent of the Financial Intelligence Agency.

9.61 The Financial Intelligence Agency may provide consent. Under Section 44 of POCA 1997 and Section 12 of ATFA 2004, a person does not commit a money laundering or terrorist financing offence if, prior to carrying out the transaction or activity, he makes an external report to the Financial Intelligence Agency and later carries out the transaction or activity with the express consent of the Financial Intelligence Agency.

9.62 RFIs may also regard as having received consent form the Financial Intelligence Agency if they do not receive notice of refusal from the FIA and/or where the moratorium period has expired. However, RFIs should contact the Financial Intelligence Agency before proceeding with a transaction or activity and receive guidance regarding information that can be provided to the customer in relation to any delay in or enquiries into the carrying out the transaction or activity. Any guidance provided by the Financial Intelligence Agency does not constitute legal advice.

9.63 Where a transaction or activity giving rise to knowledge or suspicion of money laundering or terrorist financing has been completed, a person does not commit an offence if after doing the act (or after information about the doing of the act comes to his attention) and on his own initiative he makes an external report as soon as it is reasonable for him to make it. This principle applies equally to an employee of an RFI who makes an internal report to the Reporting Officer about his knowledge or suspicion, in accordance with the RFI's policies, procedures and controls, provided that the report is made on his own initiative as soon as it is reasonable for him to make it.

9.64 Consent applies only where there is prior notice to the Financial Intelligence Agency of the transaction or activity. The Financial Intelligence Agency cannot provide consent after the transaction or activity has occurred.

Requests for additional information

9.65 Under Article 16 of the Financial Intelligence Agency Act 2007, the Financial Intelligence Agency may, in the course of enquiring into a suspicious transaction or activity relating to money laundering or terrorist financing, serve a notice in writing on any person requiring the person to provide the Financial Intelligence Agency with such information as it may reasonably require for the purpose of its enquiry.

9.66 A person who is required to provide information must provide the information to the Financial Intelligence Agency in such manner as the Financial Intelligence Agency requires.

9.67 To the extent possible, the Financial Intelligence Agency will supply, upon request from competent authorities and through planned initiatives, information as to the general status of investigations emanating from external reports as well as more general information regarding identified trends and indicators of ML/TF.

Registry of reports and enquiries

9.68 RFIs should maintain one or more registries containing record of the following:

- Reports of all enquiries made in respect of unusual transactions;
- All internal reports made to the Reporting Officer;
- Reports of all enquiries made in respect of internal reports;
- The reasons why any internal report was not reported externally to the Financial Intelligence Agency;
- All external reports made to the Financial Intelligence Agency; and
- All communications, enquiries, notices, directions and expressions of consent from the Financial Intelligence Agency related to external reports made to the Financial Intelligence Agency.

9.69 Each registry should include:

- The date of the report;

- The name of the person who made the report;
- The names of any person who added comments to the report;
- The name of the recipient of the report; and
- A reference by which all related and supporting documentation may be identified and located.

9.70 The information in the registries may be required to supplement the initial external report or serve as evidence of good practice and best endeavours in the case that there is an investigation and the suspicions are either confirmed or disproved.

9.71 The records in the registry or registries must be retained in accordance with the guidance provided in **Chapter 11**.

Transactions following a disclosure

9.72 RFIs must remain vigilant for any additional transaction or activity by a customer in respect of which an external report has been made. Additional external reports must be made where there is knowledge or suspicion that the additional transaction or activity involves the proceeds of crime, or that a person is involved in money laundering or terrorist financing.

Declining or terminating business

9.73 It is normal practice for RFIs to turn away proposed business that they know is or suspect might be criminal in intent or origin. In such circumstances, RFIs must also make an external report to the Financial Intelligence Agency, regardless of whether a transaction or activity has taken place.

9.74 RFIs should refrain from referring such declined business to other institutions.

9.75 Whether to establish or terminate a business relationship is generally a commercial decision. At times, however, the termination of a business relationship may be required by Act or Regulation, for example, under Regulation 9 where an RFI is unable to apply CDD measures in accordance with the Regulations.

9.76 The consent of the Financial Intelligence Agency for an RFI to carry out a transaction or activity is not intended to override normal commercial judgement. Consent from the Financial Intelligence Agency provides a defence against a charge of committing a money laundering or terrorist financing offence under Sections 44 and 45 of POCA 1997 and Sections 5 through 8 of ATFA 2004. Consent on its own does not create an obligation to continue a relationship.

9.77 Where an RFI decides to terminate a relationship after making an external report to the Financial Intelligence Agency, and the RFI has reason to be concerned that terminating the relationship may tip-off the customer or otherwise prejudice an investigation, the RFI should first liaise with the Financial Intelligence Agency.

9.78 Where there is continuing suspicion about a customer, transaction or activity, and there are funds that need to be returned to the customer at the end of the relationship, RFIs should seek guidance from the Financial Intelligence Agency before returning the funds.

9.79 The practices described in paragraphs 9.73 through 9.78 above are consistent with international best practice.

Tipping-off

9.80 Section 47 of POCA 1997 and Section 10 of ATFA 2004 contain tipping-off offences.

9.81 It is an offence if a person knows or suspects that an internal or external report has been made to the Reporting Officer or to the Financial Intelligence Agency and the person discloses to any other person:

- Knowledge or suspicion that a report has been made; and/or
- Any information or other matter likely to prejudice any investigation that might be conducted following such a disclosure.

9.82 It is also an offence if a person knows or suspects that a police officer is acting or proposing to act in connection with an actual or proposed investigation of money laundering or terrorist financing, and the person discloses to any other person any information or other matter likely to prejudice the actual or proposed investigation.

9.83 Reasonable enquiries of a customer regarding the background and purpose of a transaction or activity that has given rise to suspicion, form an integral part of CDD and on-going monitoring. Where such enquires are conducted in a manner that does not indicate any suspicion, they should not give rise to tipping-off.

9.84 Where an RFI has reason to be concerned that enquiries may tip-off the customer or otherwise prejudice an investigation, the RFI should first liaise with the Financial Intelligence Agency. Any guidance provided by the Financial Intelligence Agency does not constitute legal advice.

9.85 Where one member or office of a financial sector group has made or will make an external report to the Financial Intelligence Agency, that fact may be disclosed to another member or office of the same financial sector group provided that:

- The disclosure is for the purposes of discharging AML/ATF responsibilities and functions; and
- There are no grounds to believe the disclosure may prejudice an actual or proposed investigation.

9.86 RFIs may wish to seek legal advice to determine whether the criteria set forth in paragraph 9.85 are fulfilled.

Constructive trusts

9.87 An RFI holding funds or assets that it knows or suspects do not belong to its customer may be regarded under Bermuda law as a constructive trustee. In such a situation, the RFI is deemed to hold the property in constructive trust for the benefit of the actual owner of the property.

9.88 Where an RFI is a constructive trustee and it dishonestly transfers funds or assets away other than to the rightful owner, it may be held liable for knowingly assisting a breach of trust.

9.89 The duty to report suspicious activity and to avoid tipping-off could in certain circumstances lead to a potential conflict between the RFI's reporting responsibilities under the criminal law and its obligations under the civil law, as a constructive trustee, to a victim of a fraud or other crime.

9.90 Where an RFI has the suspicion it considers necessary to report under the money laundering or terrorist financing Acts and Regulations, the suspicion, in certain circumstances, may indicate that the RFI:

- Knows that the funds or assets do not belong to its customer; or
- Is on notice that the funds or assets may not belong to its customer.

9.91 Suspicion may not itself be enough to cause an RFI to become a constructive trustee. Case law suggests that a constructive trust will arise only where there is some evidence that the funds belong to someone other than the customer.

9.92 If, when making a suspicious activity report, an RFI knows that the funds or assets which are the subject of the report do not belong to its customer, or has doubts that they do, this fact and details of the RFI's proposed course of action should form part of the external report made to the Financial Intelligence Agency.

9.93 If the customer wishes subsequently to withdraw or transfer the funds or assets, the RFI should in the first instance contact the Financial Intelligence Agency for guidance.

9.94 Any consent that the Financial Intelligence Agency grants for the withdrawal or transfer of funds or assets, however, may not necessarily protect the RFI from the risk of committing a breach of constructive trust.

9.95 In cases of real need, it is open to an RFI to apply to the court for directions as to whether the customer's request should be met. It is unlikely that an RFI acting upon the direction of a court would later be held to have acted dishonestly such as to incur liability for breach of constructive trust.

9.96 The effective application of the CDD and on-going monitoring measures described in **Chapters 3 through 5**, including the identification of beneficial owners, can help RFIs to guard against a potential constructive trust suit arising out of fraudulent misuse or misappropriation of funds or assets.

Additional reporting obligations

9.97 In addition to the reporting obligations outlined in this chapter, RFIs should be aware of the reporting requirements under the Overseas Territories Orders in

Council, under which RFIs, in certain circumstances, have an obligation to make reports to the Governor. These obligations are explained in greater detail in **Chapter 6: Sanctions Regimes**.

CHAPTER 10 - EMPLOYEE TRAINING AND AWARENESS

Introduction

10.1 This chapter provides guidance on how an RFI can meet its AML/ATF obligations with regard to employee training and awareness.

10.2 The responsibilities of RFIs to ensure appropriate employee training and awareness are governed primarily by Regulations 16 and 18. The criminalisation of involvement with ML/TF and the requirement that employees report knowledge or suspicion of ML/TF are set forth in Sections 43-46 of POCA 1997 and Sections 6-8 and Schedule 1 Part 1 of ATFA 2004. The tipping-off offences relevant to an RFI's employees are set forth in Section 47 of POCA 1997 and Section 10A of ATFA 2004.

10.3 RFIs must take appropriate measures to ensure that relevant employees:

- Are aware of the Acts and Regulations relating to ML/TF;
- Undergo training on how to identify transactions which may be related to ML/TF; and
- Know how to properly report suspicions regarding transactions that may be related to ML/TF.

10.4 Each RFI must also ensure that relevant employees receive appropriate training on its AML/ATF policies and procedures relating to:

- Customer due diligence measures
- On-going monitoring
- Record-keeping
- Internal control
- Risk assessment and management

10.5 An RFI's training programme should be on-going, and should take into consideration the risks the RFI has identified through its business risk assessment. An RFI should ensure that employees receive appropriate training as their job functions and work sites change.

10.6 For the purposes of these guidance notes, the term employee includes any person working for an RFI, including persons working under a contract of employment and persons working under a contract for services. A relevant employee is one who:

- At any time in the course of his duties has or may have access to any information which may be relevant in determining whether funds or assets are the proceeds of crime, or that a person is involved in money laundering or terrorist financing; or
- At any time plays a role in implementing and monitoring compliance with AML/ATF requirements.

10.7 Temporary employees carrying out relevant functions must also receive appropriate training.

10.8 Where employees of any Bermuda-based third parties carry out relevant work in relation to an RFI under an outsourcing agreement, those employees should be aware of and trained to follow the AML/ATF policies and procedures.

Employees based in a country or territory other than Bermuda

10.9 Where operational activities of a Bermuda RFI are undertaken by employees in other jurisdictions, whether in branches, subsidiaries, representative offices or third party service providers, those employees should be aware of and trained to follow the AML/ATF policies and procedures that are applicable to Bermuda employees. For additional information on the application of group policies, see paragraphs 1.57 through 1.69.

Legal obligations on employees

10.10 Several offenses under POCA 1997 and ATFA 2004 directly affect the employees of an RFI:

- The various offenses of money laundering and terrorist financing (see paragraph 1.24);
- Failure to report knowledge or suspicion of money laundering or terrorist financing (see paragraphs 9.56 through 9.57); and
- Tipping-off and disclosure of information (see paragraphs 9.80 through 9.86).

10.11 These offenses apply to all employees. They are not directed only to those who work directly with customers but apply equally to "back office" and all other employees.

10.12 Senior management should ensure that employees receive regular and on-going training on the Acts and Regulations and guidance notes relating to ML/TF.

Employee training programme

10.13 Employees are a key component of any RFI's AML/ATF compliance programme. The effective application of even the best designed AML/ATF policies, procedures and controls can be compromised quickly if the employees implementing the compliance programme are not adequately trained. The effectiveness of an RFI's training is therefore integral to the success of the RFI's AML/ATF compliance programme.

10.14 Each RFI should develop and implement an employee training programme to ensure that all relevant employees are aware of their AML/ATF obligations and understand how to properly perform their job functions.

10.15 The training program should be approved by senior management, which is responsible for assessing its adequacy, accuracy and completeness.

10.16 Each relevant employee should receive training to ensure awareness of:

- The Acts, Regulations and guidance notes relating to ML/TF;
- The employee's responsibilities under the RFI's AML/ATF policies, procedures and controls;
- The ML/TF threats the business faces;
- The vulnerabilities of the RFI's products, services and delivery channels;
- The consequences to the RFI, its employees personally and its clients, of a breach of the Acts, Regulations or guidance relating to ML/TF;
- How to identify transactions which may be related to ML/TF;
- The identity and responsibilities of the Reporting Officer; and
- How to properly report suspicions regarding transactions or conduct that may be related to ML/TF.

Employee alertness to higher risks and suspicious activity

10.17 RFIs should ensure that relevant employees understand the RFI's approach to risk assessment and risk mitigation. Training should be tailored to the AML/ATF policies, procedures and controls that relate to employees' specific job functions.

10.18 RFIs should ensure that relevant employees receive training on how to identify and deal with customers who present a higher risk of ML/TF. Training should address the RFI's risk tolerance for such customers, and the specific risk mitigation measures the RFI has put in place, developed and documented.

10.19 RFIs should also ensure that relevant employees receive training on the vulnerabilities the RFI faces due to its products, services and delivery channels. Employees should understand and know how to apply the risk mitigation measures the RFI has developed and documented with regard to specific combinations of customers, products, services and delivery channels. For additional information, see paragraphs 2.60 through 2.66.

10.20 Employees should understand how ML and TF operate, and how these crimes might take place in connection with the RFI. RFIs should consider providing employees with case studies and examples of ML/TF related to the RFI's business.

10.21 Employees should be aware of the RFI's approach to assigning risk ratings to customers, business relationships and occasional transactions. Employees should also understand any norms that the RFI may establish for transactions and customer conduct, and procedures for identifying and scrutinising persons or activities that fall outside of those norms. For additional information regarding the use of the risk-based approach for the purposes of establishing norms and on-going monitoring, see **Chapter 7: On-Going Monitoring**.

10.22 RFIs must train relevant employees to recognise unusual or suspicious transactions or conduct, and to properly report suspicions of ML/TF.

10.23 The circumstances giving rise to unusual transactions or conduct, and which may give rise to knowledge or suspicion of ML/TF, depend on the specific combination of customer, product, service and delivery channel in question.

10.24 The following is a non-exhaustive list of transactions and conduct that may be unusual and may give rise to knowledge or suspicion of ML/TF:

- Transactions which have no apparent purpose, which make no obvious economic sense or which involve apparently unnecessary complexity;
- The use of non-resident accounts, companies or structures in circumstances where the customer's needs do not appear to support such economic requirements;
- A transaction or pattern of transactions that is, without reasonable explanation, out of the ordinary range of services normally requested or is inconsistent with the experience of the RFI in relation to the particular customer;
- Dealing with customers not normally expected in that part of the business;
- Transfers to and from high-risk jurisdictions, without reasonable explanation, which are not consistent with the customer's declared foreign business dealings or interests;
- A transaction that is structured just below the "occasional transaction" threshold to avoid CDD requirements;
- A customer who enters into a business relationship with the RFI but uses the relationship for a single transaction for only a very short period of time or after a long period of dormancy;
- Unnecessarily routing funds through third party accounts; and
- Unusual investment transactions without an apparently discernible profitable motive.

10.25 The following is a non-exhaustive list of unusual conduct that may arise during the process of identifying, verifying or obtaining additional information from a customer:

- A customer who refuses or appears particularly reluctant to provide the information requested without reasonable explanation;
- A customer who is unable or unwilling to explain a client entity's legal and corporate structure, ownership or control;
- A customer who provides information that is inconsistent or in conflict with other information the RFI holds;
- A customer who provides an address that appears vague or unusual, such as that of an accommodation agency, a professional 'registered office' or a trading address;
- A customer who opens an account or relationship in a jurisdiction that appears

inconsistent with the customer's known business;

- A customer with other business relationships with the RFI and for whom customer information, transactions or conduct are inconsistent across the different relationships;
- A customer who wants to conclude arrangements with unusual urgency against a unsatisfactorily explained promise to provide information at a later stage; and
- A customer who suggests changes to a proposed arrangement in order to avoid providing certain information.

10.26 Paragraphs 10.24 and 10.25 above provide examples only. Each RFI should ensure that it provides sufficient training to employees regarding possible indicators of unusual or suspicious transactions and conduct. The training should be specific to the RFI's business and should be kept up to date as risks constantly evolve.

Training methods and assessment

10.27 Relevant employees should be made aware of their personal responsibilities and those of the RFI at the start of their employment. These responsibilities should be documented in such a way as to enable employees to refer to them as and when appropriate throughout their employment.

10.28 Procedures manuals, whether paper or intranet based, are useful in raising the awareness of employees and in providing a day-to-day reference. However, they are not generally written as training materials and RFIs should consider the development or procurement of academically-recognised solutions.

10.29 Regardless of the training solutions used, on-going training should be given at appropriate intervals to all relevant employees. Particularly in larger RFIs, this may take the form of a rolling programme.

10.30 Each RFI should establish comprehensive records to monitor who has been trained, when they received the training and the nature of the training given. An RFI should also periodically test the knowledge and understanding of its employees, particularly on matters that are higher-risk or less-frequently encountered.

CHAPTER 11 - RECORD-KEEPING

Introduction

11.1 This chapter provides guidance on record-keeping procedures appropriate for an RFI to meet its obligations in respect of countering ML/TF. RFIs are generally required to maintain appropriate records and controls outside of the AML/ATF area; this guidance is not intended to replace or interpret those general obligations.

11.2 The record-keeping obligations of RFIs are governed primarily by Regulations 15 and 16.

11.3 Record-keeping is an essential component of establishing an audit trail. Proper record-keeping enables AML/ATF processes to keep criminal funds out of the financial system and, when required, detect criminal funds and ensure their confiscation by the authorities. Proper record-keeping also serves to demonstrate the work RFIs have undertaken in complying with their legal and regulatory obligations.

11.4 An RFI's record-keeping procedures should be sufficient to permit reconstruction of individual transactions so as to provide, where necessary, evidence for prosecution of criminal activity.

11.5 To comply with the Regulations and these Guidance Notes, the records an RFI keeps should be such that:

- The RFI's managers and auditors will be able to assess the effectiveness of the RFI's AML/ATF policies and procedures;
- Any transactions or instructions effected via the RFI on behalf of any particular customer can be reconstructed;
- The audit trail for funds entering and leaving Bermuda is clear and complete;
- Any customer can be properly identified and located;
- A customer profile can be established for all customers for whom there is a business relationship;
- All suspicions identified internally and all SARs made externally can be understood; and

- The RFI can satisfy, within a reasonable time frame, any authorised information requests or court orders from the appropriate authorities.

Timing

11.6 RFIs must keep specified records for a period of at least five years following the date on which the business relationship ends or in the case of an occasional transaction, following the date on which the transaction or the last in a series of transactions is completed.

11.7 Where a SAR is made to the Financial Intelligence Agency, whether during or after the end of any business relationship or transaction, all related specified records must be kept for at least five years following the making of the SAR.

11.8 Where a law enforcement agency notifies the RFI that particular records are or may be relevant to an investigation, the RFI must retain such records until the relevant law enforcement agency has notified the RFI that the investigation has been closed.

11.9 An RFI must establish and maintain policies, procedures and controls that enable it to respond fully and rapidly to enquiries received from the Financial Intelligence Agency or law enforcement relating to:

- Whether it maintains or has maintained during the previous five years, a business relationship with any person; and
- The nature of that relationship.

Specified records to retain

Customer due diligence

11.10 RFIs must retain all records obtained in the course of conducting CDD. Such records include those obtained during the application of both initial and on-going CDD measures. Records relating to verification of identity should comprise a copy of any official identity document(s) or if such a copy is not readily available, the information contained in the official identity document and information reasonably sufficient to obtain a copy of the document.

11.11 Where an RFI has received a confirmation of identity certificate, the RFI should keep the certificate, together with a copy of the RFI's methods used to verify identity and all verification documents obtained.

11.12 To ensure that the objectives of paragraph 11.5 are met, RFIs should maintain records concerning:

- Data obtained through the application of CDD measures;
- Copies or records of official identification documents;
- Customer verification documents;
- Customer-related data obtained from any reliable and independent source;
- Information obtained during a customer visit to an RFI's agent or premises;
- Information obtained for the purposes of enhanced CDD or on-going monitoring;
- Verification information as to beneficial ownership;
- Information concerning the purpose and intended nature of the business relationship; and
- Account files and correspondence.

Transactions

11.13 RFIs must retain all records obtained in the course of carrying out transactions on behalf of or with a customer. To satisfy the requirement that RFIs maintain a satisfactory audit trail and customer profile, transaction records should be kept of the following:

- The volume of funds flowing through the account;
- The origin of the funds;
- The form (e.g. cheque, wire transfer, etc.) and currency in which the funds were received or withdrawn;
- The identity of the person undertaking the transaction;
- The name and address (or identification code) of the counter party;
- The destination of the funds;
- The form of instruction and authority;
- Whether the transaction was a purchase or a sale;
- The account details from which the funds were paid (including, in the case of cheques, bank name, sort code, account number and name of account holder);
- Any security dealt in, including price and size;

- Any original vouchers not returned to the customer or the customer's agent; and
- Any large item/exception reports created in the course of transaction monitoring.

Other records

Training

11.14 With respect of AML/ATF training, an RFI's records should include:

- Dates AML/ATF training was given;
- The nature of the training;
- The name(s) of the person(s) giving the training;
- The names of the employees who received training; and
- The results of the tests undertaken by employees, where appropriate.

Internal and external reports

11.15 With respect to internal and external reports, an RFI's records should include:

- The results of any account or transaction-related analysis;
- Reports by the Compliance Officer to senior management;
- Records of consideration of internal compliance reports and of actions taken as a consequence;
- Where no SAR was made to the Financial Intelligence Agency, records of the material that was considered;
- Copies of any SAR made to the Financial Intelligence Agency; and
- Money laundering or terrorist financing enquiries from the authorities.

Retrieval of records

11.16 Regardless of whether a transaction was undertaken by paper or electronic means, the record retention requirements are the same.

11.17 Records, including copies of original documents, may be kept in hard copy or electronic format, so long as RFIs can retrieve them without delay.

11.18 Where records are held outside of Bermuda, it is the responsibility of the

Bermuda RFI to ensure via due diligence, contracting and periodic testing that the records are retrievable without delay and do in fact meet Bermuda legal requirements.

11.19 No confidentiality, secrecy, privacy or data protection restrictions should prevent access to the records either by the Bermuda RFI freely upon request or by Bermuda law enforcement agencies under court order. If it is found that such restrictions exist, the RFI should notify the BMA, and copies of the records should be obtained and retained in Bermuda.

11.20 RFIs should ensure that appropriate policies, procedures and controls are in place to protect the integrity and confidentiality of the records it maintains. Where data is stored in either primary or back-up form, RFIs should ensure that policies, procedures and controls are in place to detect promptly any data breach.

Third parties and financial sector groups

11.21 Where an RFI has relied upon or entered into an outsourcing arrangement with a third party, the RFI is responsible for ensuring that the third party complies with the record-keeping obligations under the Regulations and these Guidance Notes.

11.22 During the termination of a third party reliance situation or of an outsourcing arrangement, an RFI should ensure that it obtains and retains all appropriate records or oversees their transfer to another designated third party.

11.23 Where one member of a financial services group ceases to trade or have a business relationship with a customer and where the customer relationship continues with other members of the financial sector group, RFIs should take particular care to retain or hand over all appropriate records. RFIs should make similar arrangements where a company holding relevant records ceases to be part of the financial sector group.

11.24 Where relevant records are held by one member of a financial sector group, they do not need to be held in duplicate form by another member, provided the RFI has assured itself via due diligence, contracting and periodic testing that it can retrieve the records without delay.

11.25 RFIs involved in mergers, take-overs or internal reorganisations should ensure

that all relevant records are retrievable without delay throughout the transition.

ANNEX I - SECTOR-SPECIFIC GUIDANCE NOTES FOR TRUST BUSINESS

AML/ATF Sectoral Guidance Notes for Trust Business have been issued.

ANNEX II - SECTOR-SPECIFIC GUIDANCE NOTES FOR INSURANCE BUSINESS

AML/ATF Sectoral Guidance Notes for Long-Term Insurers have been issued.

ANNEX III -SECTOR-SPECIFIC GUIDANCE NOTES FOR INVESTMENT BUSINESS

AML/ATF Sectoral Guidance Notes for Investment Business have been issued.

ANNEX IV - RISK FACTORS FOR POLITICALLY EXPOSED PERSONS

IV.1 This annex contains a non-exhaustive list of risk factors relating to politically exposed persons (PEPs).

Risk factors relating to a PEP's attempt to shield his or her identity

IV.2 PEPs are aware that their status as a PEP may facilitate the detection of illicit behaviour. As a result, PEPs may attempt to shield their identity to prevent detection. Examples of ways in which this is done are:

- The use of legal entities and legal arrangements to obscure the beneficial owner;
- The use of legal entities and legal arrangements without a valid business reason;
- The use of intermediaries where doing so falls outside of normal business practices or where the use of intermediaries appears to be shielding the identity of a PEP; and
- The use of family members or close associates as beneficial owners.

Risk factors relating to a PEP's conduct

IV.3 A PEP's conduct may increase the risks associated with a business relationship or transaction. Examples include:

- The use of legal entities and legal arrangements to obscure ownership or the involvement of a particular person, industry or jurisdiction;
- A PEP inquiring about an RFI's AML/ATF or PEP policies, procedures or controls;
- A PEP who is unable or reluctant to provide information establishing the source of wealth or source of funds;
- Information provided by a PEP that is inconsistent with publicly available information, such as asset declarations or published official salaries;
- A PEP who is unable or reluctant to explain the reason for doing business in the jurisdiction of the RFI;
- A PEP who provides inaccurate or incomplete information;
- A PEPs who seeks services from an RFI that would normally not cater to foreign or high value clients;

- The repeated transfer of funds to and from jurisdictions with which the PEPs does not appear to have ties;
- A PEP who has been denied a visa or entry to the country or territory; and
- A PEP who is from a country or territory that prohibits or restricts citizens from holding accounts or owning certain property in a foreign country.

Risk factors relating to a PEP's position or involvement in business

IV.4 The position that a PEP holds and the manner in which the PEP presents his or her position are important factors to be taken into account. Possible risk factors include:

- A PEP with access to or authority over state funds, assets, policies or operations;
- A PEP with control over regulatory approvals, including the awarding of licences and concessions;
- A PEP with the formal or informal ability to control mechanisms established to prevent or detect ML/TF;
- A PEP who actively downplays the importance of his or her public function;
- A PEP who does not provide all his or her titles or positions, including those that are *ex officio*;
- A PEP with access to, or control or influence over, government or corporate accounts;
- A PEP who owns or controls, in part or in whole, any financial institution or DNFBP, either privately, or *ex officio*; and
- A PEP who is a director or beneficial owner of a legal person or arrangement that is a customer of an RFI.

Risk factors relating to the industry with which the PEP is involved

IV.5 A connection with a high-risk industry may further increase the risk of doing business with a PEP. Whether an industry poses an increased risk depends on an RFI's risk assessments and the nature of any international sanctions in effect. Examples of higher risk industries include:

- Arms trade and defence industry;
- Banking and finance;

- Businesses active in government procurement, *i.e.*, those whose business is selling to government or state agencies;
- Construction and major infrastructure;
- Development and other types of assistance;
- Human health activities;
- Mining and extraction;
- Privatisation; and
- Provision of public goods, including utilities.

Risk factors relating to a business relationship or transaction

IV.6 Risk factors may relate to a specific business relationship or transaction. Examples of such risk factors include:

- The submission of multiple STRs with regard to a PEP or a business relationship involving a PEP;
- The consistent use of rounded transaction amounts, where such use falls outside of the norm for the expected business;
- Large deposits or withdrawals into or from an account, using cash, bank cheques or other bearer instruments;
- Another RFI's termination of a business relationship with a PEP;
- Another RFI's exposure to regulatory action due to a business relationship with a PEP;
- Difficulty distinguishing between a person's personal and business money flows;
- Financial activity that is inconsistent with legitimate or expected activity;
- The movement of funds into or out of an account or between financial institutions without a business rationale;
- An account with unexpected and/or substantial activity after a dormant period, over a relatively short period, or shortly after commencing a business relationship;
- An account featuring unusual cash or wire transfer transactions;
- Transactions between non-client corporate vehicles and the PEP's account(s);
- A PEP who is unable or reluctant to provide details and credible reasons for establishing a business relationship or conducting a transaction;

- A PEP who receives large international funds transfers in a gaming account from which the PEP withdraws a small amount for gaming purposes and withdraws the balance by way of cheque or wire transfer;
- A PEP who uses third parties to exchange gaming chips for cash and vice versa with little or minimal gaming activity; and
- A PEP who uses multiple bank accounts with no apparent commercial or other legitimate reason.

Products, services, transactions and delivery channels

IV.7 Examples of products, services, transactions and delivery channels, which are of a higher risk, include:

- Private banking;
- Anonymous transactions, including cash and NPMs;
- Non-face-to-face business relationships or transactions;
- Payments received from unknown or un-associated third parties;
- Businesses that cater mainly to high value foreign clients;
- Trust and company service providers;
- Wire transfers to and from a PEP's account that cannot be economically explained, or that lack relevant originator or beneficiary information;
- Correspondent and concentration accounts;
- Dealers in precious metals and precious stones, or other luxurious goods;
- Dealers in luxurious transport vehicles, such as cars, sports cars, ships, helicopters and planes; and
- Brokers, agents and dealers working with high-end real estate.

Geographic risk factors

IV.8 Examples of higher risk geographic factors that should be taken into account when doing business with a PEP include:

- A foreign or domestic PEP from a higher risk jurisdiction, particularly where the PEP has control or influence over decisions affecting the jurisdiction's AML/ATF system;
- Foreign or domestic PEPs from a jurisdiction identified by credible sources as having a higher risk of corruption;

- Foreign or domestic PEPs from a jurisdiction that has not signed and ratified or has not sufficiently implemented relevant anti-corruption conventions, such as the UN Convention Against Corruption and the OECD Anti-Bribery Convention;
- Foreign or domestic PEPs from a jurisdiction with economic dependency on one or several export products, particularly where the jurisdiction has put in place export control or licensing measures;
- Foreign or domestic PEPs from a jurisdiction that is dependent on the export of illicit goods, such as drugs;
- Foreign or domestic PEPs from a jurisdiction with a political system that is based on personal rule, an autocratic regime, or high levels of patronage appointments, or a political system the major objective of which is to enrich those in power;
- Foreign or domestic PEPs from a jurisdiction with poor and/or opaque governance and accountability; and
- Foreign or domestic PEPs from a jurisdiction identified by credible sources as having high levels of organised crime.

ANNEX V - REGULATORY AND SUPERVISORY RESPONSIBILITIES IN BERMUDA

V.1 Bermuda Monetary Authority

Bermuda's financial regulator, with objectives and responsibilities including:

- Monitoring AML/ATF regulated financial institutions to ensure full compliance with Bermuda's AML/ATF framework;
- Assisting with the detection and prevention of financial crime;
- Deterring and criminal and terrorist activity by increasing the risk that perpetrators will be detected and by lowering the reward that perpetrators receive; and
- Issuing guidance to AML/ATF regulated financial institutions supervised for compliance with the AML/ATF regulations.

V.2 Bermuda Police Service

Bermuda's investigative body responsible for investigating all criminal activity in Bermuda, which includes money laundering, acts of terrorism and terrorist financing.

V.3 Financial Intelligence Agency:

Bermuda's financial intelligence agency, which receives reports concerning suspicions of money laundering and terrorist financing. The Financial Intelligence Agency collates, analyses and where appropriate, disseminates reports to law enforcement for investigation.

V.4 HM Customs

Bermuda's first line of defense in border control, which is responsible for:

- Interdicting illicit drugs and contraband;
- Monitoring the movement of passengers and cargo;
- Monitoring cash declarations on export or import;
- Monitoring the cross border movements of currency and bearer negotiable instruments; and

- Enforcing compliance with Bermuda's Customs laws and regulations.

V.5 **National Anti-Money Laundering Com**mittee

A Bermudian inter-governmental committee, which was established under Section 49 of the Proceeds of Crime Act 1997 for the purpose of:

(a) Advising the Minister in relation to the detection and prevention of money laundering, and on the development of a national plan of action to include recommendations on effective mechanisms to enable the competent authorities in Bermuda to coordinate with each other concerning the development and implementation of policies and activities to combat money laundering, and;

(b) Advising the Minister as to the participation of Bermuda in the international effort against money laundering.

The Chairman of the Committee is appointed by the Minister of Justice and must be a person with relevant experience. The Committee meets on a regular basis to carry out its duties. The members of the Committee are:

- The Chairman;
- The Solicitor General;
- The Financial Secretary;
- The Commissioner of Police;
- The Director of the FIA;
- The Chief Executive Officer of the Bermuda Monetary Authority;
- The Director of Public Prosecutions;
- The Permanent Secretary Ministry of Justice;
- The Collector of Customs;
- The National Coordinator;
- The Registrar General;
- The Registrar of Companies (including when acting in his capacity as Superintendent of Real Estate); or
- Such other persons as the Minister may from time to time appoint.

V.6 **Department of Public Prosecutions**

Bermuda's department responsible for prosecuting all types of crime in Bermuda, including money laundering and terrorist financing.

ANNEX VI–Corporate Service Provider Business

AML/ATF Sectoral Guidance Notes for Corporate Service Provider Business have been issued.

ANNEX VII–MONEY SERVICE BUSINESS

AML/ATF Sectoral Guidance Notes for Money Service Business have been issued.

ANNEX VIII–DIGITAL ASSET BUSINESS

AML/ATF Sectoral Guidance Notes for Digital Asset Business have been issued.