BMA
BERMUDA MONETARY AUTHORITY

BERMUDA

GUIDANCE NOTES FOR AML/ATF REGULATED FINANCIAL INSTITUTIONS ON ANTI-MONEY LAUNDERING AND ANTI-TERRORIST FINACNING 2023 (BERMUDA MONETARY AUTHORITY) NOTICE 2023

Take notice that pursuant to section 49M of the Proceeds of Crime Act 1997, the Attorney-General and Minister of Legal Affairs and Constitutional Reform has approved the Guidance Notes for AML/ATF Regulated Financial Institutions on Anti-Money Laundering and Anti-Terrorist Financing 2023. 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 13th day of February 2023.

Craig Swan
Chief Executive Officer

BERMUDA MONETARY AUTHORITY

GUIDANCE NOTES

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

AUGUST 2022

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

Table of Contents

TABLE OF ABBREVIATIONS AND ACRONYMS 3
PREFACE 4
CHAPTER 1: SENIOR MANAGEMENT'S RESPONSIBILITIES AND INTERNAL CONTROLS 10
CHAPTER 2: RISK-BASED APPROACH 25
CHAPTER 3: OVERVIEW OF CDD 39
CHAPTER 4: STANDARD CDD MEASURES 45
CHAPTER 5: NON-STANDARD CDD MEASURES 69
CHAPTER 6: INTERNATIONAL SANCTIONS 101
CHAPTER 7: ONGOING MONITORING 116
CHAPTER 8: WIRE TRANSFERS 120
CHAPTER 9: SUSPICIOUS ACTIVITY REPORTING 132
CHAPTER 10: EMPLOYEE TRAINING AND AWARENESS 145
CHAPTER 11: RECORD-KEEPING 151
ANNEX I: SECTOR-SPECIFIC GUIDANCE NOTES FOR TRUST BUSINESS 156
ANNEX II: SECTOR-SPECIFIC GUIDANCE NOTES FOR INSURANCE BUSINESS 157
ANNEX III: SECTOR-SPECIFIC GUIDANCE NOTES FOR INVESTMENT BUSINESS 158
ANNEX IV: RISK FACTORS FOR PEPS 159
ANNEX V: REGULATORY AND SUPERVISORY RESPONSIBILITIES IN BERMUDA 163
ANNEX VI: CORPORATE SERVICE PROVIDER BUSINESS 165
ANNEX VII: MONEY SERVICE BUSINESS 166
ANNEX VIII: DIGITAL ASSET BUSINESS 167

TABLE OF ABBREVIATIONS AND ACRONYMS

AML/ATF	Anti-Money Laundering/Anti-Terrorist Financing
ATFA	Anti-Terrorism (Financial and Other Measures) Act 2004
ATM	Automated Teller Machine
Authority	Bermuda Monetary Authority (also referred to as the BMA)
BACS	Bankers Automated Clearing Services
BEI	Business Entity Identifier
BIC	Bank Identifier Code
BMA	Bermuda Monetary Authority (also referred to as the Authority)
CDD	Customer Due Diligence
CHAPS	Clearing House Automated Payment System
CFATF	Caribbean Financial Action Task Force
DABA	Digital Asset Business Act 2018
EU	European Union
FATF	Financial Action Task Force
FIA	Financial Intelligence Agency
FSIU	Financial Sanctions Implementation Unit
GN	Guidance Notes for Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) Regulated Financial Institutions on AML/ATF
IBAN	International Bank Account Number
IT	Information Technology
LEI	Legal Entity Identifier
ML/TF	Money Laundering/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
POCR	Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008
RFI	AML/ATF Regulated Financial Institution
SAR	Suspicious Activity Report
POCA SEA	Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008
SWIFT	Society for Worldwide Interbank Financial Telecommunication
UK	United Kingdom
UN	United Nations

PREFACE

1. Bermuda has long-standing obligations for Regulated Financial Institutions (RFI) to maintain effective procedures to prevent and detect Money Laundering/Terrorist Financing (ML/TF). The offence of ML was first set out in the Proceeds of Crime Act 1997 (POCA). Requirements to combat TF were first included in the Anti-Terrorism (Financial and Other Measures) Act 2004 (ATFA). 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 (POCR).

2. The acts and regulations described above established a new regulatory regime. The Financial Intelligence Agency Act 2007 created the Financial Intelligence Agency (FIA) to receive and analyse Suspicious Activity Reports (SAR). The Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 (POCA SEA) designated the Bermuda Monetary Authority (Authority or BMA) as the supervisory body empowered to secure RFIs' compliance with POCR and obliges the BMA to publish these *Guidance Notes for Anti-Money Laundering and Anti-Terrorist Financing Regulated Finacial Institutions on Anti-Money Laundering and Anti-Terrorist Finaning* (GN) . The National Anti-Money Laundering Committee (NAMLC), established under Section 49 of POCA, plays an important role in developing Bermuda's national plan of action to combat ML and advises on the development and enhancement of the AML/ATF legislative framework. Additional information is available at: https://www.gov.bm/what-is-namlc.

3. Following an International Monetary Fund review of Bermuda's AML/ATF regime in 2007, a Mutual Evaluation Review by the Caribbean Financial Action Task Force (CFATF) in 2018, and revisions to the Financial Action Task Force (FATF) Recommendations in 2012 and subsequent years, further amendments to the acts and regulations were adopted in 2015, 2016, 2017 and 2018. These amendments have broadened the range of persons subject to Bermuda's AML/ATF requirements and granted additional powers to the BMA and other supervisory authorities to enforce compliance with the acts and regulations.

4. To assist RFIs in understanding and complying with Bermuda's AML/ATF acts and regulations, the BMA issued comprehensive guidance notes in January 1998, October 2010 and January 2016. GN, issued in 2022, replace and supersede earlier guidance notes. Sector-specific guidance notes that are issued from time to time and that are incorporated by reference in the GN supersede earlier versions addressing the same activities.

5. To assist RFIs and other relevant persons in structuring their own ML/TF risk assessment programmes, the NAMLC publicly released a report on Bermuda's national assessment of ML/TF risks in May 2018.

6. The BMA has hosted several outreach sessions with persons in the financial services industry to foster awareness of RFIs' obligations and of the information and processes designed to assist RFIs in complying with their AML/ATF obligations.

7. 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 the GN

8. The purpose of the GN is to assist AML/ATF RFIs, as that term is defined in Section 42A (1) of POCA, to comply with Bermuda's AML/ATF legal and regulatory framework. The GN:

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

9. Against the backdrop of Bermuda's AML/ATF laws and regulations, the GN set out guidelines for Bermuda RFIs operating both in and outside Bermuda and their connected parties, including directors, officers and employees.

10. This document provides guidance to RFIs on:

   a) The responsibilities of senior management and internal controls (Chapter 1);
   b) The risk-based approach (Chapter 2);
   c) The application of standard and non-standard Customer Due Diligence (CDD) measures (Chapters 3, 4 and 5);
   d) Sanctions regimes (Chapter 6);
   e) Ongoing monitoring (Chapter 7);
   f) Wire transfers (Chapter 8);
   g) Suspicious activity reporting (Chapter 9);
   h) Employee training and awareness (Chapter 10); and
   i) Record-keeping (Chapter 11).

What is money laundering?

11. ML 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.

12. ML 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 and criminal property.
2) Layering: The separation of 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 ML in which the criminal proceeds re-enter the legitimate economy, appearing to be derived from a legitimate source.

13. Under Bermuda law, ML involves criminal property, which under Section 2 of POCA is property that constitutes a person's benefit from criminal conduct. Criminal conduct includes all offences triable on indictment before the Supreme Court (Court). Criminal conduct also includes all offences outside Bermuda that, had they occurred in Bermuda, would be triable on indictment before the Court. For more information, see Section 3 of POCA and Section 8 of ATFA.

14. The activities carried out at all stages of the ML process are criminalised under Bermuda laws by virtue of Sections 43 through 45 and 49AA of POCA and Section 8 of ATFA. Sections 32, 33 and 230 of the Criminal Code also criminalise any attempt, conspiracy or incitement to commit any such offence.

15. Specific ML offences under Bermuda law include:

a) Concealing or transferring criminal property;
b) Assisting another to retain criminal property;
c) Acquiring, possessing or using criminal property; and
d) Importing or exporting proceeds of criminal conduct.

16. In addition, Sections 46, 47 and 49J of POCA criminalise the following acts:

a) Failure to promptly disclose to the FIA information giving rise to knowledge, suspicion or reasonable grounds for suspicion of ML;
b) Tipping off a person other than the FIA by disclosing information likely to prejudice an investigation into ML; and
c) Failure to comply with a requirement imposed under a direction issued by the Minister of Legal Affairs and Constitutional Reform.

17. Examples of ML include:

a) The attempt to turn money raised through criminal activity into legitimate or clean money;
b) Involvement with any criminal or terrorist property, or entering into arrangements to facilitate the retention or control of criminal or terrorist property; and
c) The investment of criminal property in further criminal activity or financial products and services.

18. Regardless of whether ML actually takes place, it is also a separate offence under the POCR for RFIs to fail to establish adequate and proportionate policies and procedures to prevent and detect ML.

19. The techniques used by money launderers constantly evolve, responding to the source, type

and amount of criminal property 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 practised commonly around the globe. One source of guidance on global ML methods is available at www.fatf-gafi.org.

What is terrorism financing?

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

21. TF 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 or 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.

22. 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 natural persons may operate on a smaller scale but, nonetheless, with devastating effects. TF has two notable features:

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

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

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

25. Specific TF offences under Bermuda law include:

    a) Fundraising for the purposes of terrorism;
    b) Soliciting, collecting or providing money or other property for the purposes of financing terrorist organisations or financing persons participating in terrorism;
    c) Using or possessing money or other property that is intended to be used for the purposes of terrorism; and

d) Participating in arrangements to make money or property available for the purpose of terrorism.

26. In addition, Chapter II of ATFA criminalises the following acts:

a) Failure to disclose to the FIA knowledge, suspicion or reasonable grounds for suspicion of TF;
b) Tipping off a person other than the FIA by disclosing information likely to prejudice an investigation into TF; and
c) Failure to comply with a requirement imposed under a direction issued by the Minister of Legal Affairs and Constitutional Reform.

27. Examples of TF include:

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

28. Regardless of whether or not TF actually takes place, it is also a separate offence under POCR for RFIs to fail to establish and maintain appropriate and risk-sensitive policies and procedures to prevent, detect and report TF.

29. 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 natural persons and legal entities.

30. An important component of Bermuda's ATF system is the implementation of international sanctions against groups, entities and natural persons designated as terrorists. For more information on international sanctions, see **Chapter 6: International Sanctions.**

Who does the guidance address?

31. The GN are addressed to AML/ATF RFIs within the meaning of Section 42A(1) and Schedule 3 of POCA, as referenced by Regulation 2(1) of POCR. These definitions include not only traditional financial institutions but also insurance managers, relevant insurance marketplace providers and brokers, money service businesses, corporate service providers, trust businesses, operators of investment funds, digital asset businesses, lending and leasing businesses, private trust companies and other undertakings carrying out specified financial activities. The GN are also addressed to any group that the Minister of Legal Affairs and Constitutional Reform designates as a financial group pursuant to Section 42B of POCA.

32. Approved by the Minister of Legal Affairs and Constitutional Reform, the GN are issued by the BMA under Section 5(2) of the POCA SEA.

33. The GN are of direct relevance to all senior management and compliance and reporting officers in RFIs. The primary purpose of the GN is to provide guidance to those who set the RFI's risk management policies and procedures for the prevention and detection of ML/TF.

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

Status of the guidance

35. The Court, or the BMA, 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 Legal Affairs and Constitutional Reform and issued by the BMA. Requirements of the court and the BMA are detailed in the provisions of Section 49A of POCA, Regulation 19(2) of POCR, Section 12B of and paragraph 1(6) of Part I of Schedule I to ATFA and Section 20(6) of POCA SEA.

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

How should the guidance be used?

37. This guidance interprets the laws and regulations of Bermuda to assist RFIs in meeting their AML/ATF obligations. The GN do not address every requirement. RFIs must, therefore, rely first and foremost on the laws and regulations themselves. If there is a discrepancy between these GN and any applicable legal requirements, the provisions of the legal requirement prevail.

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

39. Each RFI 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.

40. The BMA expects RFIs to address their risk management in a thoughtful and considered way and to establish and maintain policies, procedures and controls that are appropriate and sensitive to the risks identified.

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

42. When a provision of the acts or regulations is directly described in the text of the guidance, the GN use the term **'must'** to indicate that the provision is mandatory.

43. In other cases, the guidance uses the term **'should'** to describe how the BMA expects an RFI to meet its legal and regulatory obligations while acknowledging an RFI may meet its obligations via alternative means, provided that those alternatives effectively accomplish the same objectives.

CHAPTER 1: SENIOR MANAGEMENT'S RESPONSIBILITIES AND INTERNAL CONTROLS

Introduction

1.1 This chapter provides guidance for senior management to establish adequate and appropriate AML/ATF policies and procedures in line with Bermuda's acts and regulations.

1.2 The responsibilities of an RFI's senior management are governed primarily by POCA, POCA SEA, ATFA and Regulations 16-19 of POCR.

1.3 This chapter also provides guidance on internal controls relating to financial 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 Part 3 of the Regulations.

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

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

a) Assess the ML/TF risks the RFI faces. This assessment should take into account relevant findings in Bermuda's most recently published ML/TF national risk assessments;
b) Consider how those risks can be addressed most effectively; and
c) 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, an RFI may draw upon experience, applying proportionate, risk-based policies across different aspects of its business.

1.8 Under a risk-based approach, RFIs must identify and document the risks they face and assign risk ratings to their customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and transactions. AML/ATF policies, procedures and controls should be applied to allocate compliance resources proportionately to the risks identified; this approach is intended to increase efficacy in a cost-effective manner. See **Chapter 2: Risk-Based Approach**.

1.9 Senior management must ensure that the RFI's risk ratings and risk mitigation policies, procedures and controls take into consideration the results of Bermuda's most recently published ML/TF national risk assessments.

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

a) Revenue Act 1898
b) Criminal Code Act 1907
c) Taxes Management Act 1976
d) Criminal Justice (International Cooperation) (Bermuda) Act 1994
e) Proceeds of Crime Act 1997
f) Proceeds of Crime (Designated Countries and Territories) Order 1998
g) The Extradition (Overseas Territories) Order 2002
h) International Sanctions Act 2003
i) Anti-Terrorism (Financial and Other Measures) Act 2004
j) Financial Intelligence Agency Act 2007
k) Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008
l) Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008
m) Anti-Terrorism (Financial and Other Measures) (Business in Regulated Sector) Order 2008
n) Proceeds of Crime Appeal Tribunal Regulations 2009
o) The Terrorist Asset-Freezing etc. Act 2010, (Overseas Territories) Order 2011, (An unofficial consolidation of the Terrorist Asset-Freezing etc. Act 2010 (these orders are provided on the website for ease of reference)
p) International Sanctions Regulations 2013
q) Digital Asset Business Act 2018
r) Guidance Notes for Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) Regulated Financial Institutions on AML/ATF
s) Sector-specific guidance notes for:
    i. Digital Asset Business
    ii. Money Service Business
    iii. Securities Sector
    iv. Corporate Service Provider Business
    v. Trust Business
    vi. Long-Term Insurance Business

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

a) The FATF Recommendations (as amended in June 2019); and
b) United Nations (UN) Security Council resolution 1267 (1999) and its successor resolutions and resolution 1373 (2001).

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

a) Basel Committee on Banking Supervision
   i. Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-Border Wire Transfers (May 2009)
   ii. Sound Management of Risks Related to Money Laundering and Financing of Terrorism (June 2017)
b) International Association of Insurance Supervisors
   i. Guidance Paper 5 on Anti-Money Laundering and Combating the Financing of Terrorism (October 2004)
   ii. Issues Paper on Combating Bribery and Corruption (October 2004)
   iii. Application Paper on Combatting Money Laundering and Terrorist Financing (October 2013)
   iv. Examples of Money Laundering and Suspicious Transactions Involving Insurance (October 2014)
c) International Bar Association
   i. A Lawyer's Guide to Detecting and Preventing Money Laundering (October 2014)
d) International Organisation of Securities Commissions
   i. Anti-Money Laundering Guidance for Collective Investment Schemes (October 2005)
e) Wolfsberg AML Principles
   i. Available at www.wolfsberg-principles.com
f) FATF Guidance
   i. Available at www.fatf-gafi.org

Extra-territorial matters

1.14 Where an RFI has a listing, has activities 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 Bermuda's acts and regulations, sanctions and AML/ATF measures of the other country or territory also apply to the RFI's activities. 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 advise on how much the RFI's activities may be affected in this manner.

Regulatory priorities

1.15 No single Bermuda body has overall responsibility for combating ML or TF. The division of responsibilities is described in Annex V.

1.16 Regulation of and guidance to RFIs and financial groups is provided by the BMA. The Registrar of Companies is the supervisory authority for relevant persons that are dealers in high-value goods. The Superintendent of Real Estate is the supervisory authority for relevant persons that are real estate brokers or agents. The Barristers and Accountants AML/ATF Board is the supervisory authority for regulated professional firms of lawyers or accountants

that carry out 'specified activities', as defined in section 49(5) of the Proceeds of Crime Act 1997. The Casino Gaming Commission is the supervisory authority for relevant persons that are casino operators.

1.17 The POCR apply to a range of specified RFIs and other relevant persons carrying on business in or in connection with Bermuda. POCA and ATFA criminalise ML/TF, respectively. RFIs are legally obliged to put in place effective measures to minimise the chance of involvement with criminal property or any terrorist property and to report any knowledge, suspicion or reasonable grounds for suspicion of ML/TF.

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

a) Monitor AML/ATF RFIs to ensure full compliance with Bermuda's legal and regulatory framework;
b) Assist with the prevention and detection of financial crime; and
c) Deter and disrupt criminal and terrorist activity by increasing the likelihood that perpetrators are apprehended and 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:

a) Building knowledge of commercially effective compliance strategies that drive continuous improvement; and
b) 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:

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

General legal and regulatory obligations

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

a) The board of directors (board) as a single decision-making body;
b) One or more appropriate directors;
c) A 'chief executive' who, either alone or jointly with one or more persons, is responsible under the immediate authority of the directors for the RFI's conduct of the business;

d) 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:

a) Ensure compliance with the acts and regulations;
b) Secure governing body (i.e., board) approval for the RFI's policies, procedures and controls relating to its AML/ATF obligations;
c) Ensure the ML/TF risks posed by its customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and transactions are identified, assessed and effectively mitigated;
d) Ensure that the AML/ATF risk assessment framework remains relevant and appropriate given the RFI's risk profile;
e) 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;
f) Appoint a reporting officer to process disclosures;
g) Ensure employee screening against high standards;
h) Ensure that adequate resources are devoted to the RFI's AML/ATF policies, procedures and controls;
i) Ensure appropriate training to relevant employees;
j) Ensure independent audits and periodically test the RFI's AML/ATF policies, procedures and controls for effectiveness;
k) Ensure the RFI is prepared for compliance inquiries and inspections by competent authorities, including but not limited to sample testing of customer files; and
l) Recognise potential personal liability if legal obligations are 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 POCR; fulfilling these responsibilities falls to senior management as a whole. There should be evidence that senior management actively engages in the RFI's approach to addressing its ML/TF risks. See Regulation 16 of POCR.

1.23 POCR places 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) of POCR.

1.24 The offences of ML under POCA and the obligation to report knowledge, suspicion or reasonable grounds for suspicion of possible ML affect all persons, not only RFIs. Similar offences and obligations under ATFA also affect all persons, not only RFIs. In addition, POCR requires 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 on how to recognise and deal with transactions that may be related to ML/TF. See Regulations 17 and 18 of POCR, Section 46 of POCA and Schedule 1 Part 1 of ATFA.

1.25 Where a corporate, partnership or unincorporated association is guilty of an offence under POCA and/or ATFA 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, they, 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) of POCR, Section 56 of POCA and Section 5B of ATFA.

Criminal and civil penalties and other enforcement powers

1.26 RFIs should be aware that Regulation 19 of POCR provides that failure to comply with the requirements of specified POCR Regulations is a criminal offence and carries 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 POCA SEA empowers the BMA to impose a penalty on any person supervised by the BMA in an amount of up to $10 million for failure to comply with specified POCR Regulations. For full details concerning the civil penalties process, see Chapter 4 of POCA SEA. POCA SEA 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 POCA SEA. The BMA has published an *Enforcement Guide – Statement of Principles and Guidance on the Exercise of Enforcement Powers,* which states its approach to exercising its powers.

1.28 Regulation 19(4) of POCR 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.

1.29 Sections 20A through 20I of POCA SEA grant the BMA other enforcement powers when it considers that a person has contravened a requirement imposed on it by or under POCR or has failed to comply with international sanctions requirements. Those other enforcement powers include the following powers to:

a) Issue directives;
b) Restrict an RFI's licence;
c) Revoke an RFI's licence;
d) Publicly censure a person;
e) Prohibit a natural person from performing functions in relation to an AML/ATF regulated activity; and
f) Wind up or dissolve a company or firm that is or has been a licensed entity.

1.30 Section 20H of POCA SEA grants the Court the authority to enter an injunction where there is a reasonable likelihood that any person will contravene a requirement under POCR, international sanctions obligations, or any direction or licence condition imposed by the BMA.

Formal AML/ATF policy statement

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

1.32 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.

1.33 The policy statement should also set out how senior management meets its obligations under Regulation 16 of POCR to assess and document the ML/TF risks the RFI faces and how these risks are to be managed.

1.34 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.

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

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

Guiding principles:

a) An unequivocal statement of the culture and values that have been adopted by the RFI to prevent and detect financial crime;
b) A commitment to hiring and retaining only those employees who follow the principles;
c) A commitment to ensuring that employees are appropriately trained in an ongoing and risk-sensitive manner and are knowledgeable about the acts and regulations and their obligations thereunder;
d) A commitment to ensuring that the RFI accepts and maintains only those customers whose identity has been verified;
e) A commitment to the RFI 'knowing its customers' appropriately at the time of acceptance, throughout the business relationship and before executing any payments or client instructions by taking appropriate steps to verify the customer's identity, verify control and beneficial ownership, and understand the nature of the customer's business and the purpose and intended nature of the business relationship with the RFI;
f) A commitment to periodic independent auditing to test the RFI's AML/ATF policies, procedures and controls;
g) A commitment to address shortcomings in a timely manner; and
h) A commitment to ensuring that employees promptly internally report if they have knowledge, suspicion or reasonable grounds for suspicion that a person is engaged in ML/TF.

Risk mitigation procedures:

a) A summary of the RFI's approach to meeting its obligations under Regulation 16 of POCR to assess, document and manage its ML/TF risks, including a statement of the RFI's risk tolerance;
b) Identification of specific natural persons and functions responsible for implementing particular aspects of the RFI's detailed policies, procedures and controls;

c) A summary of the RFI's procedures for carrying out appropriate due diligence, including identification verification and monitoring checks on the basis of its risk-based approach; and
d) 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.

1.37 The policy statement should be tailored to the RFI's circumstances. 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

1.38 RFIs must appoint a compliance officer, who must be at the managerial level, is appropriately qualified and trained, and is required to:

a) Ensure that the necessary compliance programme procedures and controls required by POCR are in place; and
b) Coordinate and monitor the compliance programme to ensure continuous compliance with POCR.

1.39 RFIs must also appoint a reporting officer who, under the RFI's policies and procedures:

a) Receives disclosures from the RFI's employees of any knowledge, suspicion or reasonable grounds for suspicion of ML/TF;
b) Receives access to all necessary records in a timely manner;
c) Considers employee disclosures in light of all other relevant information;
d) Makes final determinations on whether they have knowledge, suspicion or reasonable grounds for suspicion of ML/TF; and
e) Where such knowledge, suspicion or reasonable grounds for suspicion exists, makes external reports to the FIA.

1.40 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.

1.41 The RFI's senior management should ensure that the reporting officer has the autonomy to make a final decision as to whether the RFI will disclose to the FIA knowledge, suspicion or reasonable grounds for suspicion of ML/TF.

1.42 The reporting officer should have direct access to the BMA and, where appropriate, law enforcement agencies to ensure that any knowledge, suspicion or reasonable grounds for suspicion of ML/TF is properly and promptly disclosed. The reporting officer must be free to liaise with the FIA on any question of whether to proceed with a transaction.

1.43 The RFI's senior management should ensure that the reporting officer has sufficient resources, including time, employees, technology, and direct access to and support from senior management. The reporting officer must also be adequately trained. 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.

1.44 The RFI's senior management should ensure that the reporting officer has immediate access to the RFI's relevant business information, including, but not limited to:

a) CDD and ongoing monitoring records; and
b) Transaction details.

1.45 The compliance officer and reporting officer may be the same natural person.

1.46 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 roles and responsibilities. The relationship should be clearly defined and documented.

1.47 Depending on the RFI's size or the structure of a financial group, the duties of the compliance officer and/or reporting officer may be delegated to additional senior, appropriately qualified and trained natural persons 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 knowledge, suspicion or reasonable grounds for suspicion of ML/TF.

1.48 Senior management should ensure that all relevant employees of the RFI are aware of the reporting officer's identity and any deputies and that all relevant employees are aware of the procedures to follow when knowledge, suspicion or reasonable grounds for suspicion of ML/TF arises.

1.49 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 Bermuda's acts and regulations.

1.50 RFIs should notify the BMA of the name and contact information of the compliance officer, reporting officer, any deputies and 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**.

1.51 For additional information regarding the reporting officer's duties, see **Chapter 9: Suspicious Activity Reporting**.

Periodic report

1.52 At least once a year, the compliance officer should report to senior management 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 more frequently. The periodic report should contain the actions and outcomes of any relevant quality assurance, independent audit or internal audit reviews of the RFI's AML/ATF processes and the outcomes of the RFI's risk assessments.

1.53 The periodic report may also include:

a) The means by which the effectiveness of the RFI's policies, procedures and controls has been managed and tested;
b) Identification of compliance deficiencies and details of action taken or proposed to address any such deficiencies;
c) Failure to apply Bermuda requirements in branches and subsidiaries, any advice received from the BMA and details of action taken;
d) The number of internal disclosures to the reporting officer, 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 CDD reviews, ongoing monitoring reviews/projects and AML/ATF training taken by the compliance officer and reporting officer;
e) Information concerning the training programme for the preceding year, which employees have received training, the methods of training and the nature of the training;
f) Changes made or proposed in respect of new or revised acts, regulations, guidance or best practices;
g) A summary of risk assessments conducted or updated with regard to customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and transactions;
h) 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
i) Any recommendations concerning additional resource requirements to ensure effective compliance with the RFI's statutory and regulatory obligations.

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

1.55 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

1.56 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.

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

a) The nature, scale and complexity of the RFI's business;
b) The diversity of its operations, including the RFI's geographical connections;
c) Its customers;
d) The business of its customers;
e) Its business relationships;
f) Its products, services and delivery channels;
g) Its transactions, including their volume, size and frequency; and
h) The degree of risk assessed in each area of its operations.

1.58 More specific requirements for an RFI's detailed policies, procedures and controls are set forth in Regulations 16 and 17A of POCR and **Chapters 2 through 11** of these GN.

Application of group policies

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

1.60 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 Bermuda's acts and regulations.

1.61 To accomplish paragraphs 1.59 and 1.60 above, RFIs should have due regard to Regulations 12 and 12A of POCR and determine whether they are obligated to adopt group-wide AML/ATF policies and procedures.

1.62 The Minister of Legal Affairs and Constitutional Reform may designate a group of companies as a 'financial group', thus bringing all members of the group into the scope of Bermuda's AML/ATF acts and regulations.

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

1.64 Group-level AML/ATF functions must be provided with customer, account and transaction information from branches and subsidiaries where required for AML/ATF purposes, including information on transactions or customers which appear unusual and have resulted in a disclosure relating to knowledge, suspicion or reasonable grounds for suspicion of ML/TF.

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

1.66 Individual RFIs and financial groups must have access to customer, account and transaction information from branches and subsidiaries where necessary for the purposes of ongoing monitoring.

1.67 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 must ensure that all suspicious transactions or activities that give rise to knowledge, suspicion or reasonable grounds for suspicion of ML/TF and are linked with a Bermuda RFI or Bermuda person are reported to the reporting officer in Bermuda.

1.68 Where the AML/ATF standards in the country or territory hosting a branch or subsidiary are more rigorous than those required by Bermuda's acts and regulations, RFIs should ensure that those higher standards are implemented.

1.69 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 manage the risks of ML/TF effectively. See Regulation 12(2) of POCR.

1.70 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.

1.71 Where an RFI finds that additional measures are insufficient for the purposes of effectively mitigating the ML/TF risks 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. The RFI should follow any advice, recommendations or directions the BMA (or other competent authority) provides as to the action to take, including any advice, recommendation or direction that the relationship be terminated.

1.72 Additional guidance regarding reliance on third parties and outsourcing arrangements is contained in **Chapter 5: Non-Standard CDD Measures**.

Employee screening

1.73 Under Regulation 18 of POCR, an RFI's AML/ATF policies and procedures must require relevant employees to be screened against high standards, as noted in paragraph 1.76 below.

1.74 For the purposes of these GN, the term 'employee' includes any person working for an RFI, including persons working on a temporary or part-time basis, whether under a contract of employment, a contract for services or otherwise. A relevant employee is one who:

a) At any time in the course of their duties, has or may have access to any information that may be relevant in determining whether funds or assets are criminal property, or that a person is involved in ML or TF; or
b) At any time plays a role in implementing and monitoring compliance with AML/ATF requirements.

1.75 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.

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

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

1.77 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

1.78 Under Regulation 17A of POCR, each RFI must ensure that its AML/ATF policies, procedures and controls are objectively evaluated by a qualified and independent person.

1.79 An auditor is qualified if it has the requisite subject matter expertise and proficiency to competently review the RFI's AML/ATF policies, procedures and controls. Such expertise and proficiency may be evidenced by continuing training, and professional education focused on AML/ATF, including internationally recognised certifications. The Certified Public Accountant designation is an outstanding and well-respected credential, but alone it has no direct correlation with AML/ATF.

1.80 An auditor is independent if it maintains independence in mental attitude in all matters relating to the audit. Any person who is involved in establishing or performing any of the RFI's ongoing AML/ATF compliance processes should not conduct an audit, determine the scope of an audit or have the authority to alter the contents of an audit report prior to its delivery to senior management and the RFI's governing body. An RFI that seeks to use an external party to conduct an AML/ATF independent audit should evaluate the independence of the persons approving and signing the agreement with the external party, as well as the independence of the persons responsible for approving the scope of the audit. An RFI that seeks to use in-house employees to conduct an AML/ATF independent audit should evaluate the reporting lines of the audit employees and verify their independence when reporting audit results.

1.81 The independent audit function must provide for a documented audit of the RFI's AML/ATF policies, procedures and controls, including those policies, procedures and controls relating to compliance with international sanctions. RFIs must 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. The audit must be conducted at least once a year. The audit should be conducted 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.

1.82 Where appropriate, having regard to the risk of ML/TF and the size of the business, the audit may be undertaken by 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. Smaller organisations may be unable to demonstrate the requisite level of independence among their employees and may find it necessary to engage an external party to conduct an independent audit.

1.83 The audit function should:

a) Assess the reliability, integrity and completeness of the RFI's AML/ATF policies, procedures and controls, including with respect to:
    i. Risk assessment;
    ii. Risk mitigation and other measures to manage higher risks;
    iii. CDD;
    iv. Ongoing monitoring;
    v. Detecting and reporting knowledge, suspicion and reasonable grounds for suspicion of ML/TF;
    vi. International sanctions;
    vii. Record-keeping and retention; and
    viii. Reliance and outsourcing relationships;
b) Evaluate the RFI's risk assessment processes and the risk ratings the RFI has assigned with respect to its size, customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and transactions;
c) Test compliance with the relevant laws and regulations;
d) Test the AML/ATF controls for the RFI's transactions and activities, with an emphasis on higher-risk areas;
e) Assess employees' knowledge of the relevant Bermuda acts, regulations and guidance, the RFI's policies, procedures and controls and the role of each relevant employee within the RFI;
f) Assess the adequacy, accuracy and completeness of employee training and awareness programmes; and
g) Review the RFI's past audit reports to assess the efficacy with which the RFI has implemented previously recommended changes.

1.84 The audit must be documented or recorded electronically and retained in accordance with the guidance provided in **Chapter 11: Record-Keeping**.

1.85 The results of the audit should be reported directly to senior management and the RFI's governing body 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 RFIs' responsibilities to utilise the risk-based approach in meeting their AML/ATF obligations are governed primarily by Regulation 16 of POCR.

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

a) Appropriate levels of CDD measures, including whether to apply enhanced CDD;
b) Mitigation measures commensurate with the risks posed by the RFI's customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and transactions;
c) The scope and frequency of ongoing monitoring;
d) Measures for detecting and reporting suspicious activity; and
e) Whether and how to launch new products, services or technologies.

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. Risk assessments must be documented, kept up to date and approved by senior management.

2.6 Policies, procedures and controls may not always prevent and detect all ML/TF. Nevertheless, 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.

<u>The concept of risk</u>

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

a) The **threat** of an event;
b) **Vulnerability** to such a threat; and
c) 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 Bermuda's NAMLC periodically conducts 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. The governments of other jurisdictions where RFIs may operate or have customers also conduct national risk assessments and publish findings useful to industry.

2.12 Each RFI should take account of relevant findings in the national risk assessments, both of Bermuda and other jurisdictions, that affect the RFI's assessment of the ML/TF risks it faces.

2.13 Each RFI should take account of sector-specific guidance, including information about the ML/TF risk associated with particular categories of business published by the FATF or other relevant organisations.

2.14 Senior management must consider whether the RFI's risk ratings and risk management policies, procedures and controls are responsive both to any risk assessments by the RFI and to any information made available to the RFI or the public with regard to the national risk assessments of Bermuda and any other relevant jurisdictions.

Business risk assessment

2.15 Under the risk-based approach, an RFI must be able to demonstrate that it follows appropriate and documented procedures for assigning risk ratings to each new product, service or technology prior to launch, each business relationship it accepts or maintains (including any outsourcing and reliance relationships) and each occasional transaction it conducts. Sector-specific guidance issued by the BMA, FATF or other relevant organisations may be useful to RFIs in assigning risk ratings and determining appropriate mitigation measures.

2.16 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.

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

2.18 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.

2.19 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 a more granular or customised basis rather than on a generic or standardised basis.

2.20 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.

2.21 Regardless of its nature, size, turnover and complexity, each RFI must begin assessing the risks it faces either before commencing business or as soon as is reasonably practicable afterwards, ensuring that any ML/TF risks that may arise are effectively managed.

2.22 Each RFI must document its risk-related policies, procedures and controls and should ensure that the methodology and results of its risk assessments are documented, regularly reviewed and amended to keep them up to date. The independent audit, which must be conducted annually or more frequently, provides an opportunity for the RFI to consider whether its risk assessments are up to date. All related records must be documented or recorded electronically and retained in accordance with the guidance provided in **Chapter 11: Record-Keeping**.

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

2.24 Each RFI must ensure that its risk assessment methodology and the results of its risk assessments are documented, approved by senior management and readily available to be shared with competent authorities.

2.25 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.

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

1) **Identify and assess inherent risks:** Consider all relevant risk factors with regard to the RFI's customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and transactions in order to assign inherent risk ratings;
2) **Establish risk tolerance:** Determine the level of risk the business is willing to accept;
3) **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;
4) **Evaluate residual risks:** Determine the level of risk remaining after taking mitigation measures into consideration;
5) **Implement risk mitigation measures:** Apply the risk mitigation policies, procedures and controls that have been developed and documented; and
6) **Monitor and review risks:** Maintain up-to-date risk assessment information and risk ratings and regularly review, test and improve the policies, procedures and controls put in place.

1) Identify and assess inherent risks

2.27 RFIs should identify and assess the inherent risks they face with regard to customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and transactions. Risk factor considerations are located throughout **Chapter 2: Risk-Based Approach**, in paragraphs 5.45 through 5.49, **Annex IV: Risk Factors for PEPs** and at the end of each of the sector-specific guidance notes issued by the BMA.

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

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

a) Business information held by the RFI, including customer information and transaction information;
b) Publicly available information, such as that in court records or reliable media;
c) Commercially available information, such as electronic databases;
d) Local, domestic and international reports and guidance regarding ML/TF threats, vulnerabilities, trends and typologies; and
e) The results of Bermuda's national risk assessments.

2.30 These GN 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.

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

a) Threat (t)
b) Vulnerability (v)
c) Consequence (c)

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

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

2.34 Paragraphs 2.35 through 2.48 address threats, inherent vulnerabilities and likelihood. Paragraphs 2.69 through 2.76 address residual vulnerabilities and their impact on likelihood. Consequences are addressed in paragraphs 2.52 through 2.61.

Threat

2.35 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 domestic and foreign crimes that result in criminal property. 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.

2.36 An RFI should assign risk ratings to each customer based upon all information available to the RFI.

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

a) Whose identification is difficult to obtain or verify;
b) Who has been accepted with no face-to-face interaction;
c) Seeking to deposit significant amounts of cash;
d) Seeking a product or service that is unusual for such a customer;
e) With an unusually or unnecessarily complex or non-transparent ownership structure;
f) Who requests undue levels of secrecy, speed, volume or frequency when transacting;
g) 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;
h) Who is a Politically Exposed Person (PEP);
i) Who is from, in or seeking to conduct business in or through a high-risk jurisdiction;
j) With regard to whom a Suspicious Activity Report (SAR) was considered or filed;
k) Who appears in reliable media, court records or electronic databases due to alleged or proven links with criminal activity.

2.38 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

2.39 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.

2.40 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.

2.41 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.

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

a) Mask the origin or destination of funds;
b) Obscure the true identity of an actual owner or beneficiary;
c) Conduct business with higher-risk business segments or in or with higher-risk jurisdictions;
d) Carry out business for a third party; or
e) Move funds to finance terrorist acts.

2.43 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, mobile device, the internet, or through intermediaries or correspondent institutions.

2.44 Some higher-risk delivery channels may include those that involve:

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

2.45 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.

2.46 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		

2.47 RFIs should assign inherent likelihood risk ratings to each potential combination of various vulnerabilities. This involves overlaying the assessments associated with customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and transactions to assess the inherent likelihood of ML/TF occurring in connection with a particular business relationship or occasional transaction.

2.48 For example, the inherent risk rating assigned to a small domestic wire transfer initiated by a resident natural person 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

2.49 Prior to entering into any outsourcing or reliance relationship, an RFI must 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 must be factored into the decision of 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 5.131 through 5.140 and 5.144 through 5.174.

Geographic connections

2.50 When assigning risk ratings, RFIs should be cognisant of the countries and geographic areas associated with their customers, business relationships (including outsourcing and reliance relationships), services, delivery channels, products and transactions and should consider whether there is a material connection to any high-risk jurisdiction. A material connection may include:

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

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

2) Establish risk tolerance

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

2.53 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 commensurate with the risks it faces and effectively apply those measures.

2.54 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.

2.55 An RFI with a large number of high-risk customer-product combinations may have the capacity and experience to manage all of its risks effectively 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 manage the higher risk effectively. 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.

2.56 Each RFI should consider:

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

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

a) Legal consequences;
b) Regulatory consequences;
c) Financial consequences; and
d) Reputational consequences.

2.58 One way to visualise risk tolerance is to combine the likelihood risk rating assigned to a particular combination of customer, business relationship (including outsourcing and reliance relationships), country or geographic area, service, delivery channel, product or transaction with a consequence rating of high, medium or low.

2.59 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:

a) The inherent likelihood rating, which is based on a combination of customer risk and inherent vulnerability (see Step 1 of the business risk assessment cycle, in paragraphs 2.27 through 2.51); or
b) The residual vulnerability rating, which is based on a combination of customer risk and residual vulnerability (see Step 4 of the business risk assessment cycle, in paragraphs 2.69 through 2.76).

2.60 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 15-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)*				

2.61 The above designations of 'Acceptable Risk' and 'Unacceptable Risk' are for illustrative purposes only. Each RFI should make its own determinations concerning the levels of risk it finds acceptable and unacceptable.

3) Establish risk mitigation measures

2.62 An RFI must develop and document appropriate policies, procedures and controls to minimise and manage the risks it has assessed. Under Regulation 16(1)(ea) of POCR, an RFI's risk mitigation mechanisms must include:

a) Consideration of the results of the RFI's risk assessments and Bermuda's national risk assessments;
b) The ability to effectively supply information to the BMA; and
c) The application of enhanced risk mitigation measures where the RFI's risk assessments identify a higher risk.

2.63 The policies, procedures and controls must be commensurate with the identified risks.

2.64 The higher the risk an RFI faces from any particular combination of customer, business relationship (including outsourcing and reliance relationships), country or geographic area, service, delivery channel, product or transaction, the stronger and/or more numerous the mitigation measures must be.

2.65 Examples of risk mitigation measures include:

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

2.66 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.

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

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

4) Evaluate residual risks

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

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

2.71 RFIs should determine the level of residual risk for each combination of customer, business relationship (including outsourcing and reliance relationships), country or geographic area, service, delivery channel, product and transaction to which an inherent likelihood risk rating was assigned.

2.72 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.

2.73 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		

2.74 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 2 of the business risk assessment cycle, in paragraphs 2.52 through 2.61).

2.75 Where an RFI finds that the level of the 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 and where those methods prove insufficient, consider whether the RFI is required to terminate or decline the business.

2.76 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.

5) Implement risk mitigation measures

2.77 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.

2.78 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.

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

a) Risk assessment;
b) CDD measures;
c) Special measures for higher risks;
d) Ongoing monitoring;
e) Detecting and reporting suspicious activity;
f) Record-keeping and retention;
g) Training;
h) Reliance and outsourcing relationships; and
i) New products, services, practices or technologies.

2.80 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 reflect the risks and needs identified through the risk assessment process.

6) Monitor and review risks

2.81 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 regularly and each time the risk factors change.

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

a) New products, services, practices, technologies and delivery channels;
b) New ML/TF trends or typologies;
c) New regulatory guidance;
d) Changes in customer portfolios or conduct;
e) Changes in products, services and delivery channels;
f) Changes in business practices; and
g) Changes in the law.

2.83 All aspects of an RFI's AML/ATF policies, procedures and controls must be fully reviewed as part of the RFI's independent AML/ATF audit. See paragraphs 1.78 through 1.85.

2.84 As noted in paragraph 1.81, 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.

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

a) Business relationship activity to determine whether actual activity is consistent with anticipated activity;
b) Whether unusual activity was appropriately reviewed and reported;
c) Customer identification and verification information to ensure it meets the requirements of the RFI's policies, procedures and controls;
d) The willingness and ability of any third parties holding CDD verification information to provide that information immediately;
e) Whether risk assessment ratings have been assigned to all customers, including introduced customers and the adequacy of those ratings;
f) The knowledge of relevant employees and senior management.

2.86 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 CDD

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 CDD measures are governed primarily by Regulations 5, 6, 8 and 9 of POCR. Simplified and enhanced CDD measures are governed primarily by Regulations 10 and 11 of POCR.

What is CDD?

3.3 CDD measures that must be carried out involve:

a) Identifying the customer and verifying the customer's identity;
b) Identifying the beneficial owner, verifying the beneficial owner's identity and, in the case of a legal person, trust or similar legal arrangement, understanding the ownership and control structure;
c) For a customer that is a legal entity or legal arrangement, identifying the name and verifying the identity of the relevant natural person having the position of chief executive or a person of equivalent or similar position;
d) Understanding the nature of the customer's business and the purpose and intended nature of the business relationship; and
e) Collecting information about the legal powers that regulate and bind a customer that is a legal person or legal arrangement.

3.4 The extent of CDD measures must be determined using a risk-based approach, taking into account various combinations of types of customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and transactions. Higher-risk situations require the application of enhanced due diligence measures. Lower-risk situations may be eligible for the application of simplified due diligence 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 ongoing monitoring?

3.6 RFIs must conduct ongoing monitoring of the business relationship with each customer. Ongoing monitoring of a business relationship means:

a) 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;

b) Investigating the background and purpose of all complex or unusually large transactions and unusual patterns of transactions that have no apparent economic or lawful purpose and recording in writing the findings of the investigation; and
c) 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 ongoing monitoring?

3.7 The CDD and ongoing monitoring obligations under POCR are designed to make it more difficult for RFIs to be used for ML/TF.

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 ATFA, POCA and regulations relating to ML/TF.

3.9 Carrying out CDD measures and ongoing monitoring allow RFIs to:

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

3.10 This GN describes a minimum level of acceptable CDD and ongoing monitoring measures. In practice, RFIs often require additional information for the purposes of managing risks and providing products and services.

Timing of CDD measures

3.11 An RFI must apply CDD measures when it:

a) Establishes a business relationship;
b) 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;
c) Suspects ML/TF; or
d) Doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

3.12 <u>General rule</u> – without exception, RFIs must always identify the customer and any beneficial owners, the nature of the customer's business, 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 establishing a business relationship or carrying out an occasional transaction.

3.14 Exception where performing CDD measures may tip-off a customer or potential customer – where there is suspicion that a transaction relates to ML/TF and a person associated with an RFI believes that performing CDD may tip off the customer or potential customer to that suspicion, the person must not perform the CDD measures and, in lieu, the RFI must file an SAR with the FIA.

3.15 Exception for life insurance and trust beneficiaries – the identification and verification of a trust customer or life insurance policy customer must be completed before establishing the business relationship. Identification of the identity of a beneficiary of a trust or life insurance policy must take place as soon as the beneficiary is designated. Verification of the identity of the beneficiary under a trust or life insurance policy may take place at a later time, but must be satisfactorily complete at the time of any payment to the beneficiary and at the time the beneficiary seeks to exercise any right or power of control vested under the trust arrangement or life insurance policy.

3.16 Exception where essential to avoid interrupting normal conduct of business – on an exceptional basis and only where the risk of ML/TF 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:

a) Ensuring that the exception is essential to avoid interrupting normal conduct of business;
b) Establishing that there is little risk of ML/TF occurring and that any ML/TF risk that may arise is effectively managed;
c) Completing the verification as soon as practicable after the initial contact;
d) Ensuring that the business relationship or account is not closed prior to efforts to complete verification;
e) Ensuring that funds received are not passed to third parties or the account holder prior to the satisfactory completion of verification;
f) 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
g) Monitoring, using a risk-based approach, by senior management of the first and each subsequent transaction until verification has been completed.

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

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

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

3.20 Where there is knowledge, suspicion or reasonable grounds for suspicion of ML/TF, this exception is not available.

3.21 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

3.22 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:

a) 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;
b) There is knowledge, suspicion or reasonable grounds for suspicion of ML/TF in relation to the customer;
c) The customer's activities are inconsistent with the RFI's understanding of the customer's business or the purpose and intended nature of the business relationship;
d) There is a material increase in the risk rating assigned to the customer or to the products, services, delivery channels, or countries or geographic areas with which the customer engages;
e) 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 RFI or a portfolio of customers by another

3.23 Where an RFI acquires another RFI 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.

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

a) The granting RFI is an AML/ATF RFI within the meaning of Regulation 10(2) of POCR;
b) 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
c) The acquiring RFI has obtained from granting RFI the CDD information and verification documentation for each customer to be acquired.

3.25 The acquiring RFI should carry out verification of identity as soon as practicable, in accordance with the acquiring RFI's risk-based approach and the requirements for existing customers opening accounts, where any of the following occurs:

a) 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;
b) The granting RFI's CDD policies, procedures or controls cannot be checked; or
c) The customer records are not accessible by the acquiring RFI.

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

3.26 RFIs must take steps to ensure that they hold appropriate CDD information with respect to business relationships established before 1 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.

3.27 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 ongoing 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.

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

a) Risks associated with their customer base are assessed;
b) Identity of their customers and any beneficial owners is obtained and verified;
c) Nature of the customer's business and the purpose and intended nature of the business relationship are understood; and
d) Level of CDD is appropriate to the assessed risk of each business relationship.

3.29 Where a business relationship has been identified as a high-risk relationship, enhanced due diligence is required.

3.30 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 in the POCR.

3.31 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.

The requirement to cease transactions

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, then, in accordance with Regulation 9 of POCR, the RFI must:

a) In the case of a proposed account or transaction, not open the account or carry out the transaction for the customer;

b) In the case of a proposed business relationship or occasional transaction, not establish that business relationship or carry out that occasional transaction with the customer;
c) In the case of an existing business relationship, terminate the business relationship with the customer; and
d) Consider whether the RFI is required to make a disclosure to the FIA in accordance with its obligations under POCA and 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 FIA, the RFI must retain the funds until a competent authority has given consent for the funds to be transferred to another account or person.

3.35 Where funds have already been received and the RFI concludes that there are no grounds for making a report to the FIA, the RFI 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 a banking institution, or an institution engaged in equivalent activities, incorporated in a jurisdiction with no physical presence involving meaningful decision-making and management and unaffiliated with a regulated financial group.

3.38 RFIs carrying on business in Bermuda must not establish an anonymous account, anonymous passbook or account obviously in a fictitious name 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 accounts obviously in a fictitious name, 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 ML/TF risks that may arise from customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and transactions that may favour anonymity. RFIs should take appropriate measures, where risk dictates, to prevent their use for ML/TF purposes.

CHAPTER 4: STANDARD CDD MEASURES

Nature of the customer's business and purpose and intended nature of proposed business relationship

4.1 An RFI must understand the nature of the customer's business and the purpose and intended nature of each proposed business relationship or transaction. In some instances, the nature of the customer's business and 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 customer's business and the nature, purpose, size and complexity of the business relationship so that the business relationship can be effectively monitored.

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

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

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:

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

Customer identification and verification of natural persons

4.5 An RFI identifies a customer by obtaining a range of information about that customer. An RFI verifies a customer's identity 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 POCR and its standard dictionary meaning.

4.7 A customer is generally the natural person or persons with whom a business relationship is established or for whom a transaction is carried out.

4.8 The term 'business relationship' means 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 establishing a business relationship.

4.9 The term 'occasional transaction' for RFIs means a transaction carried out other than as part 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.

Natural persons as beneficial owners

4.11 A beneficial owner is normally a natural person who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. In respect of customers who are natural persons, the customer themselves 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 natural person customer is not acting on their own behalf, an RFI should make appropriate enquiries to identify and verify the beneficial owner. Where a natural person is fronting for another natural person 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, a natural person'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, requiring more than one document or data source to verify all 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:

a) The nature of the product or service sought by the customer;
b) The nature of any other products or services to which the customer may migrate without further identity verification;
c) The nature and length of any existing or previous relationship between the customer and the RFI;
d) The nature and extent of any assurances from other RFIs that may be relied upon; and
e) 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 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 a natural person's identity has been undertaken; others are issued upon request, without any such checks being carried out. There is a broad hierarchy of documents:

a) First and foremost, certain documents issued by government departments and agencies or by a court; then
b) Certain documents issued by other public sector bodies or local authorities; then
c) Certain documents issued by RFIs in the financial services sector; then
d) Certain documents issued by other RFIs subject to the POCR or equivalent legislation; then
e) Certain 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 a natural person's identity, an identification document should contain a photo of the natural person 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 natural person.

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 RFIs should ensure that each identity document is in a language that is understandable to the employee with day-to-day responsibility for reviewing the document and making determinations about its authenticity and contents. Where this is not the case, the RFI should ensure that the document is translated into a language that is understandable to the relevant employee. Where an RFI's AML/ATF independent audit or any other process requires an employee to review only a selection of documents on an occasional basis, the RFI should ensure that the selection of documents is in, or translated into, a language that is understandable to the relevant employee. The RFI should be satisfied that any translated document is a fair and true representation of the original document.

Standard identification requirements for natural persons

4.24 An RFI must identify and verify the following information in relation to each natural person:

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

An RFI may accept either physical documents, electronic information and data, or a combination of both to verify the above.

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

a) Occupation and name of employer or other sources of income; and
b) Details concerning any public or high-profile positions held.

<u>Documentary verification</u>

4.26 Where seeking to verify identity using documentary evidence, an RFI should use reliable, independent source documents, data or information.

Where using documentary evidence to verify identity of a natural person, an RFI is recommended to use either a valid government-issued document, such as a passport, national identity card or driver's licence that incorporates the natural person's full legal name and photograph and one of the following:

a) Principal residential address,
b) Date of birth,
c) Place of birth; or

d) Nationality.

An RFI may accept a government-issued document lacking a photograph, such as a birth certificate, which incorporates the natural person's full legal name. In addition, the RFI must increase the level of reliability and corroborative value of the documents with **one or more additional documents** as set out in paragraph 4.27.

4.27 Where any additional document is used for the purposes of verification, it must incorporate the natural person's full legal name and cumulatively provide both of the following:

a) Principal residential address; and
b) Date of birth.

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:

a) Instrument of a court appointment (such as liquidator or grant of probate);
b) Current land tax demand letter, bill or statement;
c) 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; and
d) Utility bill.

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

4.29 Where an employee of the RFI has visited the natural person at their principal residential address, a record of the visit may constitute a second document corroborating that the natural person lives at the address.

<u>Electronic verification</u>

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

4.31 RFIs may assess the degree to which they are satisfied with 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 a natural person.

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

4.34 Negative information, such as lists of natural persons 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 on its own, 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 of a natural person or entity's identity, RFIs should be satisfied that information supplied by the data provider is sufficiently extensive, reliable, accurate and independent of the natural person or entity. This judgement may be assisted by considering whether the provider meets all the following criteria:

a) 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;
b) It uses multiple positive information sources that can be called upon to link a natural person or entity to both current and previous circumstances;
c) It accesses multiple negative information sources, such as databases relating to deceased persons, sanctions, ML, TF and identity fraud; and
d) It has transparent processes that enable the RFI to understand what checks were carried out, what the results were and how each check performed affects the level of certainty as to the identity of a natural person or entity.

4.37 In addition, a commercial agency should have processes that allow RFIs to meet their obligations to capture and store the information used to verify an identity. Where CDD is applied using online or other electronic databases, RFIs, either themselves or through third parties that the RFI has confirmed as meeting the retrieval of records requirements in paragraphs 11.18 through 11.22, must retain record of the means by which each verification was completed and, where applicable, the data supporting each verification.

4.38 For an RFI using one or more electronic databases to be reasonably satisfied that a customer is who they say they are, the standard level of confirmation is:

a) One match on a natural person's full name and current address in one information source; and
b) A second match on a natural person's full name and either their current address or date of birth in a different information source.

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. Higher levels of confirmation may include, but are not limited to:

a) Collecting additional identity information;
b) Verifying additional aspects of identity; and/or
c) Increasing the number of data points matching with the customer's identity information.

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 satisfy 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 their 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, an 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:

a) Requiring the first payment to be carried out through an account in the customer's name with an RFI in Bermuda or a jurisdiction that imposes equivalent AML/ATF requirements;
b) Verifying additional aspects of the customer's identity or of their 'electronic footprint' (see paragraph 4.13);
c) Using a reliable, independent digital identification system that is adequately protected against internal and external manipulation or falsification to avoid creating false identities;
d) Requiring copy documents to be certified by an appropriate person;
e) Contacting the customer via telephone 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;
f) 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 the customer, which in full or in part, is required to be returned, completed or acknowledged without alteration);
g) Requiring internet sign-on following verification procedures, where the customer uses security codes, tokens and/or other passwords that have been set up during account opening and provided by mail (or secure delivery) to the named natural person at an independently verified address; and
h) Employing 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 a natural person or the product, service, delivery channel, or country or geographic area with which they transact is assessed as presenting a higher risk for ML/TF, RFIs may require additional identity information and 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, they remain the owner of the funds and remain the customer. Therefore, the identity of such a donor of a power of attorney must be verified unless the donor is an existing customer of the RFI and their identity was previously 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 their identity must 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 all the requirements for simplified due diligence are met, and 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 customer may satisfy the standard identification requirement, provided that:

a) All initial and future funds are received from a Bermuda RFI or an institution in a jurisdiction that imposes equivalent AML/ATF requirements;
b) All initial and future funds come from an account in the sole or joint name of the customer or underlying principal;
c) Payments are made solely to accounts in the customer's name (i.e., no third-party payments are allowed);
d) No payments are received from third parties;
e) No changes are made to the product or service that enable funds to be received from or paid to third parties; and
f) No cash withdrawals are permitted other than by the customer or underlying principal on a face-to-face basis where identity can be confirmed and reasons for the cash withdrawal are verified in the case of significant cash transactions.

4.50 RFIs will need to demonstrate why they considered it to be reasonable to have regard to the receipt of funds as evidence in a particular instance. RFIs must conduct and document a risk assessment before concluding 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 4.49 are no longer met, RFIs must then verify the identity of the customer and any underlying principals using the standard identification requirement and any appropriate enhanced due diligence.

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 natural persons, natural persons with a legal, mental or physical inability to manage their affairs or natural persons 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 ML 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) A letter from the head of the household at which the natural person 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;
b) A letter on appropriate business letterhead from a known nursing home or residential home for the elderly confirming the residence of the applicant;
c) 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;
d) 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
e) 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 in the name of the child 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 natural persons

4.61 A customer that is not a natural person generally involves a number of natural persons, 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 natural persons who comprise the customer and its relationship with the RFI.

4.62 At a minimum, for each customer that is not a natural person, RFIs must:

a) Identify the customer and verify its identity;
b) Gather information sufficient to understand the legal form, control structure and ownership structure of the customer, including the legal powers that regulate and bind the legal person or legal arrangement;
c) Gather information sufficient to understand the nature of the customer's business and the nature and purpose of the business relationship or transaction (see paragraphs 4.1 through 4.4);
d) Identify the beneficial owners of the customer and take adequate measures on a risk-sensitive basis to verify them;
e) Identify and verify at least one natural person having the position of chief executive or a person of equivalent or similar position; and
f) Identify and verify the identity of a person purporting to act on behalf of the customer and verify that the person is, in fact, authorised to act on behalf of the customer.

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

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

4.64 RFIs must be satisfied that they know the customer, including its beneficial owners and that they have identified, assessed and mitigated any ML/TF 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 to 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 RFIs should obtain sight of and retain record of original documents regarding evidence of ownership structure, control structure, authorisations and other powers. 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 natural persons associated with a customer, RFIs should use the same standards that apply to customers who are natural persons, 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 natural 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 natural person that the RFI deals with. RFIs should identify and verify the identity of each such natural person.

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 verify each person's identity 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 an SAR 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 natural persons

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 4.97.

4.76 For the purposes of this guidance, beneficial owners are any persons, whether natural persons, legal persons or legal arrangements, that:

a) Effectively control or own more than 25% of a customer's funds, assets, shares or voting rights; or
b) In the case of trusts or similar legal arrangements, any persons who have control over the trust, are members of a class of persons on whose main behalf the trust or other legal arrangement is set up or operates, or are entitled to a specified interest in the property of the trust or other legal arrangement; or
c) Where the RFI is a corporate service provider, any person that effectively controls or owns more than 10% of the corporate service provider's customer's funds or assets.

4.77 The meaning of 'control' and 'own' in this context should be interpreted broadly to comprise the capacity to:

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

4.78 At all times, RFIs should identify and take reasonable, risk-based measures to verify the natural persons who, either directly or indirectly via another natural person, legal person or legal arrangement, ultimately control or own more than 25% or, where the RFI is a corporate service provider, 10% of a customer's funds or assets.

4.79 Where another legal person or legal arrangement holds control or ownership, RFIs should take reasonable measures to identify and verify the natural persons who ultimately control or own that other legal person or legal arrangement.

4.80 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.

4.81 In collecting identification information on all relevant natural persons, RFIs should ensure that the information collected is sufficient for the purposes of determining whether any higher-risk persons, including but not limited to PEPs, are associated with the business relationship or transaction.

4.82 Where a customer seeks to authorise signatories who are not among the natural persons 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. The identity of each signatory should be verified.

Legal persons and corporates

4.83 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.

4.84 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 ML/TF risk.

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

a) Full name and any trade names;
b) Date and place of incorporation, registration or establishment;
c) Registered office address and, if different, mailing address;
d) Address of principal place of business;
e) Whether and where listed on a stock exchange;
f) Official identification number (where applicable);
g) Name of regulator (where applicable);
h) Nature of the customer's business;
i) Nature and purpose of the business relationship; and
j) The legal powers that regulate and bind the corporate.

4.86 For corporates not subject to paragraph 4.97, RFIs must also obtain identification information, in line with the guidance for natural persons and, where relevant, legal persons, for:

a) All directors and other persons exercising control over management of the corporate, including the natural person having the position of chief executive or a person of equivalent or similar position;
b) All persons who, directly or indirectly, ultimately own or control more than 25% or, where the RFI is a corporate service provider, 10% of the customer's property, shares or voting rights;
c) All persons who otherwise exercise significant influence or control over the corporate; and
d) All other persons purporting to act on behalf of or with the authority of the corporate or by whom a binding obligation may be imposed on the corporate.

4.87 For all corporate customers not subject to the exception described in paragraph 4.97, RFIs must verify the following:

a) Full name;
b) Date and place of incorporation, registration or establishment;
c) Official identification number (where applicable);
d) Current existence of the corporate;

e) Ownership and control structures of the corporate;
f) Subject to paragraphs 4.89, 4.90 and 4.97, the identity of all chief executives, directors, signatories and other persons exercising control over management of the corporate; and
g) The identity of all other persons purporting to act on behalf of or with the authority of the corporate or by whom binding obligations may be imposed on the corporate.

4.88 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 where the RFI is a corporate service provider, 10% of the customer's property, shares or voting rights. Additional guidance applicable to trust and corporate service providers is set forth in paragraphs 4.104 through 4.123, **Annex I: Sector-Specific Guidance Notes for Trust Business** and **Annex VI: Sector-Specific Guidance for Corporate Service Provider Business**.

4.89 Where there is a large number of directors and other persons exercising control over management of the corporate, RFIs may use a risk-based approach to determine how many of those persons and which persons to identify and verify. RFIs should document their risk-based determinations. The natural persons an RFI verifies should be those the RFI expects to hold signatory powers for the purpose of operating an account or exchange instructions. Where ML/TF risks are standard or low, RFIs should verify at least two directors or other natural persons exercising significant control over management of the corporate. Where the ML/TF 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 natural persons exercising significant control over the management of the corporate.

4.90 Where any natural person 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 natural persons exercising control over management of the corporate must be verified.

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

a) Confirming the corporate's listing on an appointed stock exchange;
b) 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;
c) Obtaining sight of and retaining record of the shareholder registry;
d) Obtaining sight of and retaining record of the corporate's certificate of incorporation; and/or
e) Obtaining sight of and retaining record of the corporate's memorandum and articles of association or equivalent constitutional documentation.

4.92 Examples of measures an RFI can take to verify the nature of a customer's business include, but are not limited to:

a) Confirming a customer's internet presence, including browsing and retaining record of a customer's web page;
b) Obtaining confirmations from reliable third parties familiar with the customer and its business;

c) Conducting a site visit to the customer's place of business; and
d) Making telephone or internet inquiries to the company to confirm the products and services it offers.

4.93 Regardless of the method(s) used, RFIs must verify all the required information. Where CDD is applied using online or other electronic databases, RFIs, either themselves or through third parties which the RFI has confirmed as meeting the retrieval of records requirements in paragraphs 11.18 through 11.22, must retain record of the means by which each verification was completed and, where applicable, the data supporting each verification.

4.94 Where RFIs are unable to complete verification using the methods contained in paragraph 4.91, 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:

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

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

a) The nature of the customer's business;
b) Persons who are chief executives, directors, signatories, beneficial owners or other persons exercising control over management of the corporate;
c) Powers or authorities assigned to such persons; and
d) Other changes to the control or ownership structures of the customer.

4.96 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., when there is a change in beneficial ownership such that a person obtains greater than 25% ownership or control).

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

4.97 Where a corporate customer's securities are listed on an appointed stock exchange, the corporate is publicly owned and it is assessed as low risk in accordance with paragraph 5.3, the RFIs may forego verifying the identity of the corporate's beneficial owners and directors, provided that:

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

4.98 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

4.99 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.

4.100 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.

4.101 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.

4.102 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 RFI or independent professional within the meaning of Regulation 14(2)(a) and (b) of POCR. 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.

4.103 Where a potential or existing customer refuses to allow the immobilisation of all bearer instruments, RFIs should terminate or decline to accept the business relationship or transaction and must consider whether any reporting requirements have been implicated.

Trusts and other legal arrangements

4.104 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.

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

4.106 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 proposed business relationship, account or transaction entails any ML/TF risk. Under Regulation 6(3A) of POCR, an RFI must include each trust beneficiary as a risk factor in determining the extent of CDD measures the RFI is required to apply.

4.107 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

4.108 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:

a) Full name of the trust or other legal arrangement;
b) Date and place of establishment;
c) Registered address;
d) Legal form, nature and purpose (e.g., discretionary, testamentary or bare);
e) Control and ownership structures;
f) Official identification number (where applicable); and
g) Legal powers that regulate and bind the trust or other legal arrangement.

4.109 In line with the guidance for natural persons and legal persons, RFIs must also obtain identification information for the following persons:

a) Any donors, settlors, grantors or other persons making the arrangement;
b) All trustees or other persons controlling or having power to direct the activities of the trust;
c) Any persons whose wishes the trustees or equivalent persons may be expected to take into account;
d) Any persons purporting to act on behalf of a trustee or equivalent person;
e) The relevant natural person having the position of chief executive or a person of equivalent or similar position; and
f) Any other parties, including protectors and enforcers.

4.110 In addition, and in line with the guidance for natural persons and legal persons, RFIs must obtain and verify identification information for all known beneficiaries at the time of disbursement, and at the time a beneficiary seeks to exercise any right of control within the meaning of Regulations 3(4) and 3(5) of POCR. Known beneficiaries of trusts and other legal arrangements include:

a) 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 of benefiting from the trust or other legal arrangement;
b) Those persons who exercise control over the property of the trust or other legal arrangement, including trustees and equivalent persons; and
c) The natural persons who are beneficial owners of any legal entity that is entitled to a specified interest in the trust property within the meaning of sections 3(4) and 3(5) of POCR.

Verifying identification information

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

a) Full name of the trust or other legal arrangement;
b) Date and place of establishment;
c) Legal form, nature and purpose (e.g., discretionary, testamentary or bare);
d) Control and ownership structures;
e) Official identification number (where applicable);
f) Legal powers that regulate and bind the trust or other legal arrangement;
g) Identity of the relevant natural person having the position of chief executive or a person of equivalent or similar position; and
h) Subject to paragraphs 4.119 and 4.120, the identity of all trustees and equivalent persons controlling or having the power to direct the activities of the trust or other legal arrangement.

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

a) Obtaining sight of and retaining appropriate record of the trust deed or equivalent instrument;
b) Obtaining sight of and retaining appropriate record of the legal powers that regulate and bind the trust or other legal arrangement;
c) 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
d) Utilising independent electronic databases.

4.113 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:

a) Any donors, settlors, grantors or other persons making the arrangement;
b) Any persons whose wishes the trustees or equivalent persons may be expected to take into account;
c) Any persons purporting to act on behalf of a trustee or equivalent person;
d) Any other parties, including protectors and enforcers; and
e) All beneficial owners, as defined in paragraph 4.76.

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

4.115 Where a trustee or equivalent person is a legal person or arrangement, RFIs should verify the legal person or arrangement, including the natural persons associated with that legal person or arrangement, as would be done for a customer with the same legal form.

4.116 Where the beneficiaries of a trust or other legal arrangement are designated by characteristics of the 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 any payment to a beneficiary and at the time any beneficiary seeks to exercise any right or power of control vested under the trust arrangement.

4.117 RFIs must verify a beneficiary's identity prior to or at the time of any payment, whether direct or indirect, to the beneficiary.

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

4.119 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 natural persons 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 natural persons 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 natural persons who are not verified as signatories should be subject to verification as if they were beneficial owners. Where the ML/TF 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.

4.120 Where any natural person 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 beneficial owners, trustees and equivalent natural persons exercising control over management of the trust or other legal arrangement must be verified.

4.121 RFIs must collect information sufficient to understand the legal powers that regulate and bind a customer that is a trust or legal arrangement. 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.

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

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

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

<u>Unincorporated businesses</u>

4.124 Unincorporated businesses, including sole traders that are not legal persons, although principally operated by a natural person, differ from natural persons in that there is an underlying business. RFIs should take into account that the underlying business is likely to

have a different ML/TF risk profile from that of a natural person. Regulation 5(e) of POCR requires RFIs to understand both the nature of the customer's business and the purpose and nature of the customer's business relationship with the RFI.

4.125 Regardless of the features of a particular unincorporated 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 ML/TF risk.

4.126 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 business:

a) Full name and any trade names; and
b) Business address.

4.127 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, where the RFI is a corporate service provider, 10% of the customer's property, shares or voting rights.

4.128 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.

4.129 Where an unincorporated 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.

4.130 Where an unincorporated business is less well known or its public profile is lesser or none, RFIs should consider the customer to be a collection of natural persons. In such cases, RFIs should verify the identity of each beneficial owner using the guidance for natural persons.

Employee pension schemes

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

4.132 An RFI may elect not to identify and verify the employees who are the ultimate beneficiaries of the scheme, if a customer is a(n):

a) Employee benefit scheme or arrangement;
b) Employee share option plan;
c) Pension scheme or arrangement;
d) Superannuation scheme; or

Similar scheme where contributions are made by an employer or by way of deductions from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

4.133 In such a situation, the principal employer, including the natural person associated with the principal employer having the position of chief executive or a person of equivalent or similar position with regard to the scheme or plan, must be identified and verified using the guidance for legal persons. The source of funds should be recorded to ensure that a complete audit trail exists where an employer is wound up. Where an RFI's customer is a service provider, such as a pension advisor, for one or more schemes, the RFI should consider whether its customer is the service provider, the underlying scheme(s), or both. Additional information about the meaning of the term 'customer' is set forth in paragraphs 4.6 through 4.8. Where an RFI's customer is a service provider and not any underlying scheme(s), it may not be necessary to conduct full CDD on any underlying scheme.

4.134 In addition, any natural person 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 natural persons and, where applicable, legal persons.

4.135 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.

4.136 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 ML/TF, this exception is not available and enhanced due diligence is required.

Non-profit organisations

4.137 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.

4.138 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.

4.139 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.

4.140 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.

4.141 In exceptional cases involving trusts and other legal arrangements, RFIs will need to treat as beneficial owners other natural persons 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.

4.142 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 natural persons.

4.143 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:

a) Full name and address;
b) Nature of the organisation's activities and objectives;
c) Purpose and intended nature of the organisation's business relationship with the RFI;
d) Countries and geographic area(s) of operation;
e) Identification information for all trustees, directors or equivalent persons; and
f) Identification information for all beneficiaries or classes of beneficiaries.

4.144 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 an organisation has registered with a government body, verification of its existence may be sought by searching an appropriate government registry.

4.145 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 ongoing regulation, registration is not in itself a guarantee of the bona fides of an organisation.

4.146 For the vast majority of non-profit organisations, there will be no natural persons, apart from trustees and equivalent persons, who are beneficial owners within the meaning of POCR. 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:

a) The charter or constitution of the organisation; and/or
b) An extract from a relevant government registry.

4.147 For some organisations, no natural person or class of natural persons 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.

4.148 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 identify and verify it using the guidance for legal persons.

4.149 Non-profit organisations have been known to be used to divert funds to TF 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:

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

4.150 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.

4.151 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 POCR

4.152 Customers that are subject to POCR or its 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 purposes, in accordance with the guidance for unincorporated partnerships and businesses. Where a customer is a professional, natural person acting as, for example, a trustee or equivalent person, the professional, natural person should be identified and verified as for any other natural person, taking into account the AML/ATF Sector Specific Guidance Notes for Trust Business.

4.153 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 CDD 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, the ownership and control structure of the customer, beneficial owners, the person having the position of chief executive or similar or equivalent position and any other persons with an ownership or controlling interest in the customer, or persons who otherwise exercise significant influence or control over the customer or its business relationship with the RFI.

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

a) Applying reduced or simplified CDD measures in accordance with the POCR and this guidance; or
b) 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 countries or geographic areas with which the customer engages. Determinations concerning the application of simplified due diligence measures must be made only after taking into account the results of Bermuda's 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:

a) The customer is a Bermudian RFI acting for its own account;
b) The customer is an RFI or equivalent institution in a country or territory outside Bermuda that meets the requirements of Regulation 10(2)(b) of POCR and is acting for its own account;
c) The customer is a company whose securities are listed on an appointed stock exchange;
d) The customer is an independent professional that meets the requirements of Regulation 10(4) of POCR, the product is a pooled account and information on the identity of the persons whose funds are held in the pooled account is available upon request to the account custodian;
e) The customer is a public authority in Bermuda;
f) The product is
    i. A life insurance contract where the annual premium is no more than $1,000 or where there is a single premium of no more than $2,500;
    ii. An insurance contract for the purpose of a pension scheme where the contract contains no surrender clause and cannot be used as collateral; or
    iii. A pension, superannuation or similar scheme which provides retirement benefits to employees, where contributions are made by an employer or by way of deduction

from an employee's wages and the scheme rules do not permit the assignment of a member's interest under the scheme; or

g) The product, service or transaction otherwise meets the requirements of Schedule (1) to POCR, including where:
   i. The product has a written contractual base;
   ii. Any related transaction is carried out through an account of the customer with a Bermudian bank or with a bank situated in a country or territory other than Bermuda that is subject to equivalent regulation;
   iii. The product or related transaction is not anonymous;
   iv. A product relates to the financing of a physical asset where the title is not transferred until the termination of the contractual relationship and annual payments do not exceed $15,000;
   v. The maximum transaction amount is $15,000;
   vi. A third party cannot benefit from the product or related transaction, except in the case of death, disablement, survival to a predetermined advanced age or similar events; and
   vii. The product involves an investment or purchase of insurance or another type of contingent claim, the benefits are realisable only in the long term, the product cannot be used as collateral, and no surrender, accelerated payment or early termination takes place during the contractual relationship;

and both:

a) The RFI has conducted and documented a risk assessment, and the RFI has reasonable grounds for believing that there is a low risk of ML/TF; and
b) The RFI has no knowledge, suspicion or reasonable grounds for suspicion of ML/TF.

5.5 RFIs should keep risk findings up to date and in writing, 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 promptly 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:

a) AML/ATF RFIs transacting solely on their own behalf (see paragraph 5.146);
b) Natural persons for whom receipt of funds may serve as evidence of identity (see paragraphs 4.49 through 4.52);

c) Natural persons for whom reduced or alternative documentation may be acceptable for the purposes of identification and verification (see paragraphs 4.53 through 4.60);
d) Companies listed on an appointed stock exchange (see paragraphs 4.97 through 4.98);
e) Employee pension schemes (see paragraphs 4.131 through 4.136); and
f) Bermuda public authorities.

5.9 RFIs contemplating reliance on a third party for the purposes of applying CDD measures should have regard to paragraphs 5.117 through 5.148 of the GN.

5.10 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.

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

a) Maintain and document up-to-date risk findings concerning the products, services, customers, business relationships (including outsourcing and reliance relationships), countries and geographic areas associated with the business;
b) Ensure that the level of CDD applied is commensurate with the assessed risks;
c) Conduct ongoing monitoring of the business relationship;
d) Report any knowledge or suspicion of ML/TF; and
e) 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.

5.12 Where an RFI assesses the risks associated with any business relationship or occasional transaction as anything other than lower than standard, where an RFI doubts the veracity or adequacy of documents, data or information previously obtained for the purpose of identification or verification, or where an RFI has any knowledge, suspicion or reasonable grounds for suspicion of ML/TF, the RFI must discontinue the application of any reduced or simplified CDD measures and apply either standard or enhanced due diligence measures, commensurate with the risks the RFI has identified.

5.13 Where there is any knowledge, suspicion or reasonable grounds for suspicion of ML/TF, or where an RFI has reason to suspect that a customer is acting to avoid the application of standard CDD measures, the RFI must also consider whether any reporting requirements have been implicated.

Enhanced due diligence

5.14 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.

5.15 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 ongoing risk assessment processes. The second is to provide a tailored basis for monitoring customer

activity and transactions, so attempts to launder money and finance terrorism are more likely to be detected.

5.16 Enhanced due diligence must be applied in all circumstances where the ML/TF 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.

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

a) The customer has not been physically present for identification purposes (see paragraphs 5.25 through 5.29);
b) The business involves a correspondent banking relationship (see paragraph 5.148);
c) The business relationship or occasional transaction involves a PEP (see paragraphs 5.96 through 5.116); or
d) The business relationship or occasional transaction has a connection with a country or territory that represents a higher risk of ML, corruption, TF or being subject to international sanctions, including but not limited to any country that has been identified as having a higher risk by the FATF or the CFATF.

5.18 A business relationship or occasional transaction has a connection with a country or territory that represents a higher risk of ML, corruption, TF or being subject to international sanctions where a person associated with the business relationship or occasional transaction is:

a) The government or a public authority within the country or territory;
b) A PEP in relation to the country or territory;
c) A person who is a resident in, citizen of or incorporated in the country or territory;
d) A person having a registered office or other business address in the country or territory;
e) 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; or
f) Transacting from or with the country or territory.

5.19 For the purposes of paragraph 5.18, a person associated with the business relationship or occasional transaction is any of the following:

a) Customer;
b) Beneficial owner or controller of the customer;
c) Third party for whom the customer is acting;
d) Beneficial owner or controller of a third party for whom the customer is acting; or
e) Person acting or purporting to act, on behalf of the customer.

5.20 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 ML/TF.

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

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

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

a) 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 in the customer, or persons who otherwise exercise significant influence or control over the customer or its business relationship with the RFI;
b) Conducting enhanced ongoing monitoring of the business relationship by increasing the number and frequency of controls applied and by identifying patterns of transactions requiring further examination; and
c) Requiring the first payment to be carried out through an account in the customer's name via an RFI subject to the POCR 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;

5.23 Where an RFI knows of or suspects ML/TF 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.

5.24 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 promptly upon request to authorised authorities.

Non-face-to-face identification and verification

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

5.26 In limited circumstances, and only where the risk of ML/TF is assessed as low, limited exceptions (see paragraphs 3.14 through 3.21) may be available.

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

a) Ensuring that the customer's identity is established by additional documents, data or information;
b) Further verifying or certifying the documents acquired, for example by obtaining confirmatory certification by an RFI subject to the POCR, 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;
c) Using a reliable, independent digital identification verification application or tool that is adequately protected against internal and external manipulation or falsification to avoid creating false identities; and
d) Requiring the first payment to be carried out through an account in the customer's name via an RFI subject to the POCR 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.

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

5.29 RFIs should at all times be cognisant 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

5.30 **Chapter 8: Wire Transfers** sets forth general guidance for RFIs that are Payment Service Providers (PSP) carrying out transfers of funds as payer PSPs, intermediary PSPs and payee PSPs.

5.31 Regulation 11 of POCR 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) A higher-risk person or jurisdiction, including any person or transaction from or in a country that has been identified by the FATF or the CFATF as having a higher risk;
b) International sanctions;
c) A customer who has not been physically present for identification purposes;
d) A non-Bermuda correspondent bank;
e) A PEP; or
f) Any other situation that, by its nature, can present a higher risk of ML/TF.

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

a) PSP's risk tolerance and risk assessments;
b) Involvement of any third-party service provider;

c) Particular nature of the transfer that has been requested, in the context of the accountholder's previous transactions and conduct.

5.33 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) A payer who is unwilling or unable to provide the required complete information;
b) A payer for whom the complete information cannot be verified, where it is required to do so;
c) 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;
d) A payer seeking to route the transaction through apparently unnecessary intermediary PSPs;
e) A payer seeking to ensure that the complete information does not reach all PSPs involved in the execution of the payment;
f) A transfer with missing, meaningless or otherwise incomplete information;
g) A transfer of funds in an amount greater than $1,000 to a non-account holder, particularly where no unique identifier accompanies the transfer;
h) 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; and
i) A transfer for which there is evidence to suggest that a person other than the named payee is the intended final recipient.

5.34 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:

a) Reject the transfer;
b) Request the complete information on the payer and payee; and/or
c) Make an internal SAR to the reporting officer.

5.35 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 8.59 through 8.61.

New payment methods

5.36 New payment methods (NPM) are recent and ongoing technological innovations in payment and value transfer systems, including, but not limited to:

a) Pre-paid cards and tokens;
b) Payments by mobile phone;
c) Internet-based payment systems; and
d) Payments, trades and transfers involving virtual currencies.

5.37 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.

5.38 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 GN. 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.

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

5.40 An initial risk assessment must 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 must also be assessed on an ongoing basis.

5.41 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 5.82 through 5.93.

5.42 Many NPMs, or the services associated with NPMs, do not fall neatly into the categories described in paragraph 5.36, 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.

5.43 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.

5.44 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

5.45 RFIs must have policies, procedures and controls in place to prevent the misuse of any business involving NPMs for the purposes of ML/TF.

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

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

5.48 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.

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

a) CDD;
b) Usage limits;
c) Geographic limits;
d) Monitoring and record-keeping; and
e) Segmentation due diligence and controls.

NPM CDD

5.50 RFIs must 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.

5.51 For general guidance on non-face-to-face identification and verification, see paragraphs 5.25 through 5.29.

5.52 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 5.82 through 5.93.

5.53 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 POCR, Regulation 9 requires the refusal or termination of the business relationship or transaction.

5.54 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 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.

5.55 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.

5.56 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.

5.57 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 8.70 through 8.71. Where appropriate or required, RFIs should obtain and verify the identity of any recipient of funds.

5.58 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 linked activity that, collectively, exceeds any threshold amount or frequency or appears abnormal or suspicious.

5.59 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.

5.60 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.

5.61 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, RFIs should monitor transactions between the NPM account and the RFI for any abnormal or suspicious activity.

5.62 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 5.82 through 5.93.

NPM usage limits

5.63 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.

5.64 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.

5.65 Examples of usage limits include restrictions on:

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

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

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

5.68 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 ongoing manner.

5.69 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 RFI. See paragraph 5.60.

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

NPM geographic limits

5.71 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.

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

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

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

5.74 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 from or in any jurisdiction where the NPM provider is not subject to adequate AML/ATF regulation and oversight.

5.75 RFIs should use IP addresses and other geolocation data 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

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

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

5.78 RFIs should use ongoing 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.

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

5.80 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 5.82 through 5.93.

5.81 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

5.82 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.

5.83 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.

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

a) Difficulty in conducting effective CDD;
b) Difficulty in conducting ongoing monitoring;
c) Loss of information, or an inability to access information;
d) Unclear lines of communication and accountability; and
e) The involvement of NPM providers not subject to appropriate registration, licensing and AML/ATF regulation requirements.

5.85 Both prior to entering into a business relationship with an NPM product or service provider and throughout any such relationship, an RFI must assess whether and how each person and jurisdiction involved in the NPM may affect the RFI's ability to fulfil its obligations under the POCR and these GN. 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.

5.86 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 ongoing due diligence for NPM providers.

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

a) Whether the NPM service provider is licensed or otherwise authorised to carry out the NPM's activities;
b) Whether, where relevant, the service provider is effectively regulated;
c) 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;

d) Whether any operational, financial, human resource, structural, legal or regulatory considerations may affect the service provider's ability to carry out effective CDD and ongoing monitoring, where relevant, or impede the RFI's access to relevant information held by the NPM service provider, including customer and transaction information;
e) 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.

5.88 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.

5.89 RFIs must not enter into a 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.

5.90 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 that NPM product or service provider, the customer agreement between the RFI and NPM provider should confirm that the RFI will receive, upon request, transaction and customer information on users of the NPM.

5.91 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.

5.92 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.

5.93 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 6.61 through 6.65.

Agent networks and other third parties

5.94 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.

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

PEPs

5.96 Natural persons, who have or have had a high political profile or hold or have held public office or a prominent function in an international organisation, can pose a higher risk to RFIs as their position may be abused for ML and related predicate offences such as corruption and bribery, as well as for the financing of terrorism and proliferation. This risk also extends to their family members and known close associates. PEP status itself does not, of course, incriminate natural persons or entities. It does, however, put the customer, beneficial owner or other person with an ownership or controlling interest in the customer, or persons who otherwise exercise significant influence or control over the customer or its business relationship with the RFI into a higher-risk category.

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

5.97 A PEP is defined in Regulation 11 of POCR. The application of AML/ATF regulations concerning PEPs also extends to members of their immediate families and known close associates.

5.98 The application of AML/ATF regulations concerning PEPs extends to the following persons:

<u>PEPs in or from any country or territory outside Bermuda:</u>

a) Heads of state, heads of government, ministers and deputy or assistant ministers;
b) Members of parliament and senior political party officials;
c) 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;
d) Members of the courts of auditors or of the boards of central banks;
e) Ambassadors, charges d'affaires and high-ranking officers in the armed forces;
f) Members of the administration, management or supervisory bodies of state-owned enterprises; and
g) Natural persons entrusted within the preceding year with prominent public functions or a prominent function by an international organisation, as defined in Regulation 2(1) of POCR, including senior management, directors, deputy directors and members of the board or equivalent function of an international organisation.

<u>PEPs in or from Bermuda:</u>

a) The Governor, Premier, Ministers and Junior Ministers;
b) Members of the Legislature;
c) Permanent Secretaries;

d) Judges of the Supreme Court and Court of Appeal and Magistrates;
e) Members of the Board or senior management of the Authority and the Regulatory Authority of Bermuda;
f) Commissioned officers in the Royal Bermuda Regiment and senior officers above the rank of Sergeant (which includes the Commissioner of Police) of the Bermuda Police Service;
g) Members of the Board of Directors and the Chief Executive Officer (by whatever name called) of the Bermuda Government-owned or controlled enterprises or authorities, including but not limited to:
   i. West End Development Corporation;
   ii. Bermuda Land Development Corporation;
   iii. Bermuda Development Agency;
   iv. Bermuda Tourism Authority;
   v. Bermuda Deposit Insurance Corporation;
   vi. Bermuda Casino Gaming Commission; and
h) Natural persons entrusted with a prominent function by an international organisation, as defined in Regulation 2(1) of POCR, including senior management, directors and deputy directors and members of the board or equivalent function of an international organisation.

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

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

<u>Family members of natural persons entrusted with the requisite public or prominent function:</u>

a) Spouse;
b) Partner (including a person who is considered by national law as equivalent to a spouse);
c) Children and their spouses or partners;
d) Parents; and
e) Siblings.

<u>Close associates of natural persons entrusted with the requisite public or prominent function:</u>

a) Natural persons known to have joint beneficial ownership of a legal entity or legal arrangement with a PEP;
b) Natural persons who have sole beneficial ownership of a legal entity or legal arrangement that has been set up for the benefit of a PEP; and
c) Natural persons known to have any other close business relations with a PEP.

Determination of PEP status

5.99 RFIs must utilise risk-based procedures to determine whether the customer or beneficial owner is a PEP in or from Bermuda or a PEP in or from a country or territory outside Bermuda.

Ongoing monitoring

5.100 RFIs are required to conduct ongoing monitoring to identify whether existing customers, beneficial owners, other persons with ownership or controlling interests or persons who otherwise exercise significant influence or control over the customer or its business relationship with the RFI have become PEPs after the initial establishment of the business relationship. Such ongoing 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 ongoing monitoring of the business relationship is provided in **Chapter 7: Ongoing Monitoring**.

Life insurance policies

5.101 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

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

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

Sources of information on PEPs

5.103 For the purpose of deciding whether a natural person 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 verification, they may rely upon a wide range of sources, including commercial databases, internet and media searches, including social media.

5.104 Where RFIs need to carry out research to determine the level of risk of the business relationship with a 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 and highlight specific issues and industries of concern. Resources such as mutual evaluation reports, which assess the compliance of countries with the international AML/ATF 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 perceived levels of corruption, may be helpful in assessing the level of risk. Actual knowledge concerning a natural person and the reputation of the natural person may also help assess the level of risk.

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 consider the limited nature of PEP databases and should use them only as additional sources of information on higher-risk natural persons 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 PEP database.

Risk-based enhanced due diligence

PEPs in or from any country or territory outside Bermuda

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

a) 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 is or has become a PEP;
b) Take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or occasional transaction; and
c) Conduct enhanced ongoing monitoring of the business relationship.

PEPs in or from Bermuda

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

a) 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 is or has become a PEP;
b) Take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or occasional transaction; and
c) Conduct enhanced ongoing monitoring of the business relationship.

Life insurance and trust beneficiaries who are PEPs

5.108 Life insurance companies and trust businesses must 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 measures, life insurance companies and trust businesses are required to:

a) Notify senior management before the pay out of policy proceeds or the exercise of a vested right; and
b) 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 1.20 of this GN. 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 the 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 1.38 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 a PEP's family member or close associate, 'source of wealth' means the origin of the person's total assets. Information on the 'source of wealth' should indicate 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, including any family member or close associate, 'source of funds' means the origin of the particular funds or other assets that are involved in the business relationship or occasional transaction. Information concerning '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 sending (or receiving) 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. Nevertheless, 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 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) and internet and media searches including social media.

Level of risk of the business relationship with a PEP in or from Bermuda

5.114 When determining whether the business relationship with a PEP in or from Bermuda should be classified as higher risk, RFIs should consider risk factors, including whether the PEP:

a) Has business interests that are related to their public function or prominent function with an international organisation;
b) Is involved in public procurement processes or international organisation procurement processes;
c) Is from a country or territory that represents a higher risk of ML, corruption, TF or being subject to international sanctions, including but not limited to a country identified by the FATF or CFATF as higher risk;
d) Has a prominent public function or prominent international organisation 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
e) Has a public function or prominent function with an international organisation that would allow them to exert a negative impact on the effective implementation of the international AML/ATF standards in Bermuda.

Enhanced ongoing monitoring

5.115 When conducting enhanced ongoing monitoring of the business relationship with a PEP, RFIs should have regard to paragraphs 5.14 through 5.24. 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.

5.116 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 5.141 through 5.143.

Multipartite relationships, including reliance on third parties

Reliance on third parties

5.117 An RFI may choose to rely upon another person or institution (a third party) to apply certain CDD measures, provided that the RFI immediately obtains information sufficient to identify customers and both the third party and the nature of the reliance meet certain other criteria. In any reliance situation, however, the relying RFI retains responsibility for any failure to comply with a requirement of the POCR, as this responsibility cannot be delegated.

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

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

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

a) The duty to conduct ongoing 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 owners, nature of the customer's business, purpose and intended nature of the business relationship and, where necessary, the source of funds or wealth; and
b) The duty to report knowledge, suspicion and reasonable grounds for suspicion of ML/TF.

5.120 RFIs may rely upon a third party that is:

<u>For Bermuda persons</u>

a) An AML/ATF RFI, as defined in Regulation 2(1) of POCR; or
b) An independent professional, as defined in Regulation 2(1) of POCR, that is supervised for Bermuda AML/ATF purposes by a designated professional body in accordance with Section 4 of POCA SEA.

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

a) An institution that carries on business in a country or territory other than Bermuda and that business corresponds to the business of an AML/ATF RFI or an independent professional. The independent professional must be subject to mandatory professional registration recognised by law; or
b) Is subject to requirements equivalent to those laid down in the POCR and supervised by a supervisory authority for compliance with those requirements.

<u>Limitations to reliance</u>

5.121 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 or product is confirmed as falling under Regulations 10(2), 10(3), 10(4), 10(5), 10(6) or 10(7) of POCR, it is not permissible to rely upon simplified due diligence.

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

5.123 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) of POCR permits simplified due diligence on the independent professional (or similar professional) only where the following conditions are met:

a) 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
b) 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

a) The pooled account is held by an independent professional (or similar professional) in a country or territory other than Bermuda that imposes AML/ATF requirements equivalent to those of Bermuda;
b) The independent professional (or similar professional) has effectively implemented those requirements and is supervised for compliance with that jurisdiction's AML/ATF requirements; and
c) 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.

5.124 RFIs may rely upon another person or institution to carry out CDD measures only when the person or institution that an RFI relies upon confirms in writing to the RFI that the person or institution has, either itself or through a properly administered outsourcing arrangement, actually applied the CDD measures.

5.125 Reliance is permissible only on the basis of the written notification and consent described in paragraphs 5.128 through 5.130 that are exchanged between a first person or institution that actually applied CDD measures and a second person or institution relying on the first person or institution; there can be no 'chain' or 'passing on' of reliance involving more than two persons or institutions. An RFI may not rely upon another person or institution to apply CDD measures where that person or institution has not in fact applied the CDD measures or is itself relying upon yet another person or institution to apply the CDD measures. Likewise, a Bermudian RFI or a non-Bermudian entity conducting business corresponding to the business of a Bermudian RFI that has relied upon another person to apply certain CDD measures may not consent to be relied upon for purposes of those same CDD measures.

5.126 For an RFI to confirm that it has carried out CDD measures in respect of a customer is a serious matter. Any improper reliance situation may preclude an RFI from accessing information it needs to appropriately assess the risks associated with a customer, transaction or business relationship. In addition, any person who fails to comply with the reliance requirements set forth in Regulation 14(1) of POCR is guilty of an offence and liable to prison or a fine of up to $750,000.

5.127 A third party consenting to be relied upon 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 and both a willingness and ability to share evidence or other records of the verification.

Notification and consent

5.128 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) of POCR. Examples of ways this notification may be delivered are:

a) When 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; and
b) 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.

5.129 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:

a) The third party, either itself or through a properly administered outsourcing arrangement, has applied the CDD measures for which the RFI is relying upon the third party;
b) The third party has not relied upon any other party to apply those CDD measures; and
c) Upon request by the relying RFI, the third party will make available copies of the verification data and other relevant documents or information on the customer, beneficial owners, nature of the customer's business and purpose and intended nature of the business relationship that the third party obtained when applying CDD measures.

5.130 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

5.131 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.

5.132 In addition to satisfying itself that the third party meets the criteria of paragraph 5.120, RFIs should consider related risk factors, including:

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

d) Whether the third party has satisfactorily responded to any previous requests to make available, without delay, information concerning the identity of any customer or underlying customer or copies of verification data;
e) 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.

5.133 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 regularly operates in or from a high-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.

5.134 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.

5.135 For reliance to be permissible, relying RFIs must obtain certain information immediately, including:

a) Identity of the customer;
b) Identity of the beneficial owners;
c) As appropriate, the nature of the customer's business and the purpose and intended nature of the business relationship; and
d) Level of CDD that has been carried out.

5.136 In practice, at the outset of the customer relationship and periodically throughout the customer relationship, RFIs will request and receive, without delay, 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 ongoing monitoring and is generally set out in the form or forms that the relying RFI will require to be completed.

5.137 At a minimum, however, relying RFIs must satisfy themselves that information on the identity of underlying customers and copies of documents, data and other information used by the third party for verification of the items listed in paragraph 5.135 are kept in accordance with the guidance provided in **Chapter 11: Record-Keeping** and 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.

5.138 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 information on the identity of underlying customers and evidence of verification. This is particularly relevant when ongoing 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, suspicion or reasonable grounds for suspicion of ML/TF is present.

5.139 Where an RFI makes such a request, and it is not met in a timely manner, 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.

5.140 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

5.141 Where customers are introduced between different parts of the same financial 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:

a) The group entity that carried out the CDD measures can be relied upon as a third party under this guidance;
b) The group has implemented group-wide AML/ATF policies and procedures that facilitate the sharing of CDD and transaction information while ensuring adequate safeguards on the confidentiality and use of the information exchanged;
c) The group entity makes available to the group the information described in paragraph 5.135;
d) 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;
e) The group's home is in Bermuda or in a jurisdiction that imposes equivalent AML/ATF requirements;
f) 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 (e.g., a relied-upon institution that has applied only simplified or standard CDD measures is not being relied upon where the relying RFI's relationship with a customer requires the application of enhanced due diligence measures).

5.142 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.

5.143 Where the verification evidence for any customer is inadequate for any reason or required for ongoing monitoring, any missing verification evidence will need to be obtained.

Situations that are not reliance

<u>A third party acting solely as an introducer</u>

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 complete, retained and accessible.

Regulated financial institutions

5.146 When a customer of a Bermuda RFI is an RFI under Regulation 10(2) of POCR 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 5.13), 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 in accordance with POCR, to the underlying customer.

Correspondent relationships

5.148 When a cross-border correspondent banking relationship exists or is being considered, in addition to conducting ongoing monitoring and reporting any knowledge or suspicion of ML/TF, RFIs must:

a) Determine from publicly 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;
b) Assess the respondent's AML/ATF controls;
c) Obtain approval from senior management before establishing new correspondent relationships (see paragraph 5.109);
d) Clearly understand the respective responsibilities of each institution; and
e) 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 immediately providing relevant CDD information to the RFI in accordance with paragraph 5.135.

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 group of which the RFI may be a member, any outsourcing arrangement is subject to the POCR and these GN. Note that the outsourcing of AML/ATF activities is carved out from the BMA's Guidance Notes on Outsourcing for Banks, Deposit Companies, the Bermuda Stock Exchange, Corporate Service Providers, Trust Companies, Money Service Businesses, Investment Businesses, Fund Administrators and the Credit Union.[1] Therefore, outsourcing relating to AML/ATF-specific activities are governed by these GN.

5.150 Outsourced activities must be carried out in accordance with the RFI's policies, procedures and controls. The RFI must have specific policies, procedures and controls for monitoring and managing any service provider to which the RFI outsources an activity relating to AML/ATF. In addition, the RFI must ensure that the service provider has in place AML/ATF systems, controls and procedures that are in compliance with Bermuda AML/ATF requirements. The governing body of the RFI must ensure clearly defined and documented roles, responsibilities and duties or persons responsible 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 POCR and these GN.

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

a) 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;
b) Impeding the effective ability of the RFI's board or similarly empowered body or natural person to provide oversight;
c) Impeding the effective ability of the appropriate regulator to monitor the RFI's compliance with all obligations under the regulatory system;
d) Reducing the responsibility of the RFI and/or its managers and officers;
e) Removing or modifying any conditions subject to which the RFI's authorisation was granted; and
f) Increasing ML/TF risk in any way that is not adequately addressed through appropriate risk assessment and mitigation.

[1] The following guidance do not address AML/ATF specific activities but rather the prudential elements: https://www.bma.bm/viewPDF/documents/2019-06-28-10-38-02-Outsourcing-Guidance-Note.pdf

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 and accountabilities that cannot be outsourced

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

a) Direct the RFI's risk policies and procedures;
b) Continuously identify, assess, monitor and manage the risks associated with outsourcing activities to the service provider;
c) Continuously supervise, monitor and test the adequacy of the activities carried out by the service provider; and
d) 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 must identify, assess, monitor and document the risks created by outsourcing the proposed activities. In particular, the RFI must assess and document whether and how outsourcing may affect its ability to fulfil its obligations under the POCR and these GN. 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 must carry out due diligence with respect to the service provider under consideration. The purpose of the due diligence is to determine whether the service provider has the ability, capacity, any required authorisation and the systems, controls and procedures to perform the outsourced activities reliably, professionally and in accordance with the POCR and these GN. RFIs must establish a written policy concerning the scope and frequency of initial and ongoing due diligence carried out with respect to such service providers.

5.160 At a minimum, RFIs carrying out due diligence with respect to a service provider should

consider the following:

a) Whether the service provider is licensed or otherwise authorised to carry out the outsourced activities;
b) Whether, where required, the service provider is effectively regulated;
c) 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;
d) 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;
e) 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;
f) Whether the service provider can maintain the confidentiality of RFI and client information; and
g) Whether the service provider has effective procedures in place 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 to use a service provider, whether the service provider is in Bermuda or outside of Bermuda, RFIs should assure their own ability to monitor the service provider effectively 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.

<u>Clear statement of functions to be outsourced</u>

5.163 The outsourcing agreement should be drafted to remove any doubt about 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:

a) Precisely define the rights and obligations of the RFI and the service provider;
b) Specify all activities being outsourced;
c) Clearly state all requirements, including regulatory obligations, concerning the service provider's performance of the outsourced activities;
d) Specify the persons at both the RFI and the service provider who are responsible for implementing, monitoring and managing the outsourcing arrangement; and

e) Specifically state the name or title of the RFI's Bermuda officer who retains ultimate responsibility for the RFI's compliance with POCR and these GN. This person is normally the compliance officer referred to in paragraph 1.38 of these GN.

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:

a) The service provider is required to report regularly to the RFI;
b) 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;
c) 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 POCR and these GN;
d) 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;
e) The RFI and service provider have clearly delineated their respective responsibilities, in accordance with POCR and these GN, for providing appropriate AML/ATF training and reporting suspicious activity. See **Chapter 10: Employee Training and Awareness**.

Access to information

5.167 For the purposes of complying with POCR, and these GN 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 operating in or from any country or territory outside Bermuda, 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 RFI to take remedial action where the service provider's performance falls short of that required by the outsourcing agreement, POCR or these GN or where a Bermuda regulatory authority orders, in writing, the RFI 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, POCR and these GN.

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 POCR and these GN. The outsourcing RFI should be required to approve in writing any changes to the subcontracting arrangements.

CHAPTER 6: INTERNATIONAL SANCTIONS

Introduction

6.1 This chapter provides guidance to assist RFIs in meeting their obligations under Bermuda's international sanctions regime.

6.2 The obligations of RFIs with respect to international sanctions are set forth primarily in the International Sanctions Act 2003 and the International Sanctions Regulations 2013.

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.

6.5 Bermuda's Financial Sanctions Implementation Unit (FSIU) has published Financial Sanctions Guidance and Financial Frequently Asked Questions that provide additional relevant information for RFIs.

6.6 Effective 25 September 2018, the International Sanctions (Delegation of Governor's Functions) Notice 2018 (BR 104 / 2018) delegated to the Minister of Legal Affairs and Constitutional Reform the authority to:

a) Obtain evidence and information;
b) Issue and revoke licences;
c) Serve as a reporting depository;
d) Authorise investigations and the collection of evidence and information pursuant to the International Sanctions Regulations 2013; and
e) Specify, in the currency of Bermuda, the equivalent amount to be taken to sums expressed in sterling in the relevant order listed in Schedule 1 of the International Sanctions Regulations 2013.

Overview of international sanctions

6.7 Financial sanctions are enforcement measures the international community uses to achieve, maintain or restore international peace and security in a specified regime. Financial sanctions are imposed on an entity, regime or natural person within a regime by the UN, EU or United Kingdom (UK) as a tool to comply with certain foreign policy or national security objectives. The effect of sanctions is to:

a) Limit the provision of certain financial services; and
b) Restrict access to financial markets, funds, goods, services and economic resources.

6.8 Financial sanctions are largely imposed to:

a) Coerce a regime or natural persons into changing their behaviour, or aspects of it, by increasing the cost on them to such extent that they decide to cease the offending behaviour;
b) Constrain a target by denying it access to key resources needed to continue its offending behaviour, including the financing of terrorism or nuclear proliferation;
c) Signal disapproval, resulting in stigmatising and potentially isolating the target, or as a way of sending broader political messages domestically or internationally; and
d) Protect the value of assets that have been misappropriated from a country until such assets can be repatriated.

6.9 Measures that are frequently applied through international sanctions include:

a) Financial sanctions, including asset freezes, bans on investment or access to capital markets, limitations on banking activities or relationships and restrictions on the provision of other financial services or advice;
b) Trade controls on the importation, exportation or financing of specified goods, services, equipment and activities; and
c) Directions to cease all business with a specific person, group, sector or country.

6.10 The primary sources of international sanctions affecting Bermuda RFIs are the UN and EU. 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 6.17 through 6.19.

Penalties for non-compliance

6.11 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, a fine or both.

6.12 RFIs must be aware that, in contrast to AML/ATF measures, which generally permit RFIs 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 natural person or entity, it may not transact with any natural person or entity subject to the Bermuda sanctions

regime without first ensuring that an appropriate licence is in effect.

6.13 The Bermuda sanctions regime applies to natural persons 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 or 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, both that person and the RFI are guilty of that offence and liable to be proceeded against and punished accordingly.

6.14 Section 5(1B) of POCA SEA grants the BMA authority to monitor RFIs for compliance with their international sanctions obligations. Section 20 of POCA SEA authorises the BMA to impose a civil penalty of up to $10 million on an RFI for any failure to comply with international sanctions obligations.

6.15 Sections 20A through 20I of POCA SEA grant the BMA other enforcement powers when it considers that a person has failed to comply with international sanctions requirements. Those other enforcement powers include the following powers to:

a) Issue directives;
b) Restrict an RFI's licence;
c) Revoke an RFI's licence;
d) Publicly censure a person;
e) Prohibit a natural person from performing functions in relation to an AML/ATF regulated activity; and
f) Wind up or dissolve a company or firm that is or has been a licensed entity.

6.16 Section 20H of POCA SEA grants the court the authority to enter an injunction where there is a reasonable likelihood that any person will contravene an international sanctions obligation or any direction or licence condition imposed by the BMA.

Other unilateral sanctions regimes

6.17 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.

6.18 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.

6.19 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 1.59 through 1.72.

The Bermuda sanctions regime

6.20 Most of Bermuda's international sanctions are brought into force through the International Sanctions Act 2003 and the International Sanctions Regulations 2013.

6.21 The Bermuda sanctions regime is based largely upon the UK's sanctions regime. The International Sanctions Act 2003 grants the Minister of Legal Affairs and Constitutional Reform authority to make regulations giving effect to any international sanctions obligation of the UK. The International Sanctions Regulations 2013 are made pursuant to that authority.

6.22 Schedule 1 of the International Sanctions Regulations 2013 lists the UK's sanctions regime-related Overseas Territories Orders in Council (Order) that have been brought into force in Bermuda.

6.23 The Minister of Legal Affairs and Constitutional Reform amends Schedule 1 of the International Sanctions Regulations 2013 to ensure that new sanctions are brought into force in Bermuda and that sanctions, once withdrawn in the UK, are retired from effect in Bermuda. Schedule 2 lists sanctions that have been revoked.

6.24 A portal to information regarding Bermuda's international sanctions requirements, including the HM Treasury's consolidated list of persons constituting the target of financial sanctions, orders in force in Bermuda and the consolidated list of restricted goods is available at www.gov.bm/international-sanctions-measures.

6.25 The scope of restrictions contained in each Order varies, and RFIs must review each Order, together with any accompanying lists, annexes, schedules, updates or amendments to ensure compliance with the Order's specific requirements. Nevertheless, most of the Orders provide for most or all of the following common restrictions:

a) Asset freezing;
b) Information gathering;
c) Reporting; and
d) Licensing.

6.26 An asset freeze generally prohibits dealings with the frozen funds or economic resources belonging to or 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.

6.27 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.

6.28 When a person is named as a sanctions target, their name is recorded on the consolidated list. Nevertheless, an asset freeze and some financial services restrictions will also apply to entities that are owned or controlled, directly or indirectly, by a sanctions target. Although entities owned or controlled by a sanctions target may not be included on the consolidated list, such entities are nonetheless subject to financial sanctions.

6.29 To assess whether a legal person or entity is owned by another person or entity, RFIs should determine whether the sanctions target owns more than 50% of the proprietary rights of an entity or has a majority interest in it. If this criterion is met, then financial sanctions apply both to the sanctions target and to the majority-owned entity.

6.30 'Owned' is interpreted to include direct and indirect ownership. If it is determined that a sanctions target is the ultimate beneficial owner of an entity, for example, where the sanctions target owns a corporate body that, in turn, owns another corporate body, then all entities that are part of the ownership chain are subject to financial sanctions.

6.31 To assess whether a legal person or entity is controlled by another person or entity, RFIs should consider whether, with regard to the legal person or entity, a sanctions target:

a) Has the right or exercises power to appoint or remove a majority of the members of the administrative, management or supervisory body of such legal person or entity;
b) Has appointed, solely as a result of the exercise of the sanctions target's voting rights, a majority of the members of the administrative, management or supervisory bodies of a legal person or entity who have held office during the present and previous financial year;
c) Controls alone, pursuant to an agreement with other shareholders in or members of a legal person or entity, a majority of shareholders' or members' voting rights in that legal person or entity;
d) Has the right to exercise a dominant influence over a legal person or entity, pursuant to an agreement entered into with that legal person or entity or to a provision in its memorandum or articles of association, where the law governing that legal person or entity permits its being subject to such agreement or provision; or

e) Has the right to exercise a dominant influence referred to in the point above without being the holder of that right, including by means of a front company.

6.32 Sanctions in effect in Bermuda require RFIs to inform the FSIU of any instance in which:

a) The RFI knows, suspects or has reasonable cause to suspect that a customer or any person with whom the RFI has or has had dealings is a sanctions target; or
b) The RFI or sanctions target has breached a sanction.

6.33 Any report described in paragraph 6.32 must be made to the FSIU, and a copy should be provided to the BMA. For additional information about sanctions-related reporting, see paragraphs 6.84 through 6.87.

6.34 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.

6.35 The FSIU has the authority to grant a licence to an RFI to engage in an activity that would otherwise be prohibited by a sanctions regime. For additional information about licensing, see paragraphs 6.90 through 6.93.

Compliance with the Bermuda sanctions regime

6.36 Each RFI must have adequate policies, procedures and controls to comply with the Bermuda sanctions regime.

6.37 An RFI's policies, procedures and controls should be documented and should be reviewed and endorsed by its governing body (e.g., board of directors).

6.38 Each RFI's policies, procedures and controls must enable it to conduct ongoing screening of its customers and transactions to determine whether it is conducting or may conduct business involving any sanctioned person, entity, activity or good.

6.39 The RFI's sanctions checking processes should be proportionate to the nature and size of its business and should be likely to identify all target matches with sanctions targets. For additional information on target matches, see paragraphs 6.80 through 6.83.

6.40 An RFI's process of determining which sanctions compliance measures are proportionate and likely to identify all target matches differs in a key manner 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, in the absence of an appropriate licence from the FSIU, is in breach of the sanctions regime and liable to be prosecuted.

6.41 Although there is no room for risk tolerance in sanctions compliance, an RFI's assessment of its risk of exposure to sanctioned persons, entities and activities is expected to assist in preventing the RFI from breaching the sanctions regime. Each RFI should conduct such a risk assessment, tconducting it in line with what is prescribed for the AML/ATF assessment in paragraph 2.22 and keeping it up to date with reference to the following non-exhaustive list of risk factors:

a) Customers, products and activities;
b) Distribution channels;
c) Complexity and volume of transactions;
d) Processing and systems;
e) Operating environment;
f) Screening processes of intermediaries;
g) Geographic risk; and
h) Any other relevant sanctions regulations.

6.42 To tailor its sanctions compliance measures to the nature and size of its business, an RFI should take the following steps:

a) Understand and identify the applicable sanctions;
b) Develop and document appropriate policies, procedures and controls in order to comply with the sanctions;
c) Apply the sanctions compliance policies, procedures and controls that have been developed and documented;
d) Maintain up-to-date sanctions information; and
e) Regularly review, test and improve the sanctions compliance policies, procedures and controls put in place.

6.43 Each RFI should ensure that its sanctions-related policies, procedures and controls effectively guide the RFI in:

a) Ensuring up-to-date knowledge of the applicable sanctions;
b) Tailoring sanctions compliance measures to the RFI's business;
c) Screening the RFI's customers, transactions, third-party service providers and geographic connections for potential matches with sanctions targets;
d) Reviewing potential matches to identify target matches;
e) Freezing assets or taking any other required action in the event of a target match;
f) Reporting target matches and any breaches;

g) Ascertaining whether any appropriate general licence is in effect;
h) Applying for and monitoring compliance with appropriate licences;
i) Ensuring appropriate staff awareness and training;
j) Documenting and recording actions taken to comply with the sanctions regime and the rationale for each such action; and
k) Reviewing the effectiveness of the RFI's policies, procedures and controls.

6.44 To ensure up-to-date knowledge of the applicable sanctions, an RFI 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.gov.bm/international-sanctions-measures.

6.45 RFIs should bear in mind that HM Treasury's Consolidated List of Targets and the lists of restricted goods linked at www.gov.bm/international-sanctions-measures may identify targets of sanctions that are not in effect in Bermuda. Where an RFI identifies a target 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 6.84 through 6.87.

6.46 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. Nevertheless, 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.

6.47 Screening customers and transactions for potential matches with sanctions targets is addressed in paragraphs 6.61 through 6.79.

6.48 Reviewing potential matches to identify target matches and reporting target matches and any breaches are addressed in paragraphs 6.80 through 6.83.

6.49 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 6.26, requirements to freeze funds and assets generally apply not only to customers but also to any other person or entity involved in a transaction, including legal persons and entities owned or controlled by 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.

6.50 Applying for and monitoring compliance with licences is addressed in paragraphs 6.90 through 6.93.

6.51 RFIs should ensure that effective policies, procedures and controls are implemented to prohibit and detect attempts by employees or customers to:

a) 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
b) Structure transactions for the purpose of concealing the involvement of a sanctions target.

Training

6.52 Each RFI should implement a sanctions-related employee training and awareness programme that is appropriate for the RFI's business.

6.53 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.

6.54 The substance of the training and awareness programme should, at a minimum, include the RFI's policies, procedures and controls for:

a) Complying with new sanctions that come into force;
b) Ceasing compliance with sanctions that have been retired from effect;
c) Screening for applicable sanctions targets;
d) Reporting target matches and any breaches;
e) Documenting actions taken to comply with the sanctions regime and the rationale for each such action; and
f) Communicating changes to the RFI's sanctions obligations, including changes to its sanctions-related policies, procedures and controls.

Documentation and record-keeping

6.55 RFIs should ensure that appropriate record is made of the following:

a) The RFI's sanctions-related policies, procedures and controls;
b) Actions taken to comply with the sanctions regime;
c) Information sought and obtained to confirm or eliminate a potential match;
d) The persons who decides whether a potential match is a target match;
e) The rationale for the decision; and
f) The information used for preparing, and contained in any report to the FSIU.

6.56 RFIs, at a minimum, should retain record of the following information about any

potential match, whether it turned out to be a true match or a false positive:

a) The information or other grounds that triggered the match (e.g., a 'hit' provided by screening software);
b) Any further checks or enquiries undertaken;
c) The relevant sanctions regime;
d) The person(s) involved, including any members of compliance or senior management who authorised treatment of the match as a false positive;
e) The nature of the relationship with the person or entity involved, including attempted or refused transactions;
f) Subsequent action taken (e.g., freezing accounts); and
g) Whether the RFI consulted with or filed a report with the FSIU.

6.57 All related records should be retained in accordance with the guidance provided in **Chapter 11: Record-Keeping**.

Reviewing effectiveness

6.58 Each RFI should monitor its policies, procedures and controls to ensure full, up-to-date and timely compliance with rapidly changing sanctions obligations.

6.59 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 1.78 through 1.85.

6.60 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:

a) Oversee the establishment, maintenance and effectiveness of the RFI's sanctions-related policies, procedures and controls;
b) Monitor compliance with the relevant acts, regulations and guidance; and
c) Access all necessary records in a timely manner in order to respond to any information gathering authorised by an order.

Screening customers and transactions

6.61 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.gov.bm/international-sanctions-measures.

6.62 RFIs should screen not only their customers but, wherever possible, any other related parties, including, but not limited to, the following:

a) Counterparties;

b) Trustees and similar persons;
c) Beneficial owners, directors, signatories and similar persons of customers, counterparties and third-party service providers;
d) Persons authorised by power of attorney; and
e) The geographic connections of the abovementioned persons and entities.

6.63 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 CDD Measures** and **Chapter 5: Non-Standard CDD Measures**.

6.64 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.

6.65 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 8.25 through 8.66.

Timing and scope of screening

6.66 Initial screening of customers and related parties should take place during the establishment of a business relationship or as soon as possible thereafter.

6.67 Where an RFI conducts screening after the establishment of a business relationship, it should be aware that it risks transacting with a sanctions target in breach of the sanctions.

6.68 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.

6.69 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.

Screening software

6.70 RFIs may choose to use commercially available screening software; other RFIs may rely on manual screening.

6.71 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.

6.72 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.

6.73 Where automated software screening is used, RFIs should monitor and test the ongoing effectiveness of the software and ensure that adequate contingency arrangements are in place in the event that the software fails.

'Fuzzy matching'

6.74 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 misspelt, 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.

6.75 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

6.76 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 the introduced business has been screened for sanctions compliance or that any screenings conducted were adequate or maintained up to date.

6.77 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. RFIs should satisfy themselves that the service provider is providing an effective service.

6.78 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.

6.79 In contemplating any reliance or outsourcing relationship with a third party, RFIs should have due regard to paragraphs 5.117 through 5.174.

Reporting matches and breaches

6.80 RFIs should investigate potential matches with sanctions targets to determine whether there are any target matches.

6.81 A target match arises where an RFI knows, suspects or has reasonable grounds to suspect that it is conducting or may conduct business involving a sanctions target. For additional information on the meaning of 'knowledge,' 'suspicion' and 'reasonable grounds for suspicion,' see paragraphs 9.7 through 9.19.

6.82 An RFI may need to seek sufficient information from relevant parties to enable it to determine whether it has knowledge, suspicion or reasonable grounds for suspicion of a target match. An RFI should ensure that there is a clear rationale for any decision that a potential match is not a target match.

6.83 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.

6.84 RFIs must ensure that they have clear internal and external reporting processes for reporting target matches to the FSIU and the BMA. These reporting processes may involve the reporting officer and should be designed with due regard to the guidance provided in paragraphs 9.22 through 9.49.

6.85 Where an RFI identifies a target 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.

6.86 Where an RFI identifies a target match for sanctions that are in effect in Bermuda, the RFI must:

a) Immediately comply with the terms of the order by immediately freezing any funds or economic resources, where required, or taking any other required action; and

b) Not enter into financial transactions or provide financial assistance or services in relation to the sanctions target, and not engage in any other activity sanctioned under the order unless either:
   i. There is an exemption in legislation on which the RFI can rely;
   ii. There is an applicable general licence in effect; or
   iii. The RFI has obtained an applicable specific licence from the FSIU; and

c) Immediately report the target match in writing to the FSIU at:

The Minister of Legal Affairs and Constitutional Reform
Financial Sanctions Implementation Unit
4th Floor, Global House
43 Church Street
Hamilton, HM12
Bermuda

Telephone: (441) 292-2463

E-mail: fsiu@gov.bm

In addition, RFIs should complete the Compliance Reporting Form available in Annex 2 of the FSIU's Financial Sanctions Guidance as soon as possible after reporting the target match to the FSIU.

Where an RFI has already reported details of accounts, economic resources or other funds held frozen for sanctions targets, it is not required to report these details again. If there are details of any other involvement with a listed natural person or entity, directly or indirectly, or of any attempted transactions involving those natural persons or entities, this should be reported to the FSIU.

6.87 When informing the FSIU of a target match or that an RFI or a sanctions target has breached a sanction (see paragraph 6.25), the RFI should copy the BMA at aml@bma.bm and include the following:

a) The information or other matter on which the knowledge, suspicion or reasonable grounds for suspicion or breach is based;
b) Any information held by the RFI about the sanctions target by which the target can be identified; and
c) The nature and amount, quantity or value of any funds or economic resources held by the RFI in relation to the sanctions target.

6.88 Where an RFI freezes assets, it should do so immediately upon discovering the target match and should ensure that relevant staff do not process any further transactions without an express direction from senior management.

6.89 Where a target match is identified before commencing a business relationship, an RFI should not accept the business unless it first confirms that an applicable general

licence is in effect or it first applies for and obtains an appropriate specific licence.

Licensing

6.90 An RFI may apply for a specific licence 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 sanctions.

6.91 If a specific licence is granted, it will normally be accompanied by a letter stating the purpose of the licence being issued and the precise scope of the activity the licence authorises.

6.92 RFIs may also verify whether any applicable general licence that would permit an action otherwise prohibited by sanctions has been issued.

6.93 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 applicable licence that is in effect.

Suspicious activity reports

6.94 Holding an account for a sanctions target or processing a transaction which involves a sanctions target is not in itself grounds for filing a SAR with the FIA.

6.95 Nevertheless, where an RFI has knowledge, suspicion or reasonable grounds for suspicion that funds or assets involve criminal property, the RFI must comply with its suspicious activity reporting obligations under the acts and regulations.

Customer notification and tipping-off

6.96 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 and ATFA, informing customers or third parties of a target's sanctions status is not a tipping-off offence.

6.97 By contrast, where an RFI has filed an SAR with the FIA, disclosing the fact that the SAR was filed is a tipping-off offence. See paragraphs 9.82 through 9.88 for additional information on tipping-off offences.

CHAPTER 7: ONGOING MONITORING

Introduction

7.1 This chapter provides guidance for the requirement that RFIs conduct ongoing monitoring of the business relationships with their customers.

7.2 The responsibilities of RFIs to conduct ongoing monitoring are governed primarily by POCR Regulations 7, 6(3), 6(3A), 11(4)(c), 12(1)(b), 13(4), 14(A)(2)(d), 14(A)(3), 16 and 18.

7.3 RFIs must conduct ongoing monitoring of the business relationship with their customers. An RFI may not utilise a reliance situation to delegate to another financial institution the RFI's duty to conduct ongoing monitoring. Nevertheless, an RFI may seek to outsource ongoing monitoring appropriately.

7.4 Ongoing monitoring is an integral part of an RFI's AML/ATF programme and supports several objectives:

a) Maintaining a proper understanding of a customer's activities;
b) Ensuring that CDD documents and other records are accurate and up to date;
c) Providing accurate inputs for the RFI's risk assessment processes;
d) Testing the outcomes of the RFI's risk assessment processes; and
e) 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 Ongoing monitoring of a business relationship includes:

a) Scrutinising transactions undertaken throughout the course of the relationship (including, where necessary, the source of wealth and/or source of funds) and other aspects of the business relationship to ensure that the transactions and customer's conduct are consistent with the RFI's knowledge of the customer and their risk profile;
b) 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;
c) Determining whether a customer is a PEP;
d) Determining whether a customer relationship involves a country or territory that represents a higher risk for ML, corruption, TF or being subject to international

sanctions, including but not limited to a country that has been identified by the FATF or CFATF as being higher risk;

e) Reviewing existing documents, data and information to ensure that they are up to date, adequate and relevant for the purpose of applying CDD measures; and
f) Adjusting risk profiles and risk assessments based on information reviewed.

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 3.22.

7.8 RFIs should determine the scope and frequency of ongoing monitoring using a risk-based approach. RFIs should direct greater monitoring resources toward those products, services and business relationships presenting a higher risk of ML/TF than 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 ML/TF.

7.9 In determining a proper allocation of monitoring resources, RFIs should consider the:

a) Size and complexity of the RFI;
b) Nature, scope and delivery channels of the products and services the RFI provides;
c) Most recently published ML/TF national risk assessments;
d) RFI's own risk assessment findings; and
e) Nature, scope and effectiveness of the RFI's existing monitoring systems.

7.10 With respect to the customer, RFIs should consider:

a) The nature, amount and frequency of the transactions;
b) Geographic connections (see paragraph 2.50);
c) Whether the customer is known to use other products and services;
d) 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
e) Whether the customer presents a higher than standard risk for ML/TF.

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 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 any person seeking 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 the business conducted by many RFIs, cash transactions may be relatively uncommon, whereas for many banks, credit unions or money services businesses offering services to local customers, cash transactions may be a normal everyday 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:

a) Transactions and conduct are flagged in exception reports for further examination;
b) The exception reports are reviewed promptly by the appropriate person(s); and
c) Appropriate and proportionate action is taken to reduce the possibility of ML/TF occurring without detection.

7.16 An RFI should calibrate its monitoring systems to identify for review all higher-risk activity, including:

a) All complex or unusually large transactions and unusual patterns of transactions which have no apparent economic or lawful purpose;
b) Transactions or conduct falling outside of the expected norm for a customer, product or service; and
c) Transactions or conduct involving any of the circumstances described in paragraphs 5.16 through 5.19.

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. Each 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 ongoing 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:

a) The system sufficiently monitors for appropriate ML/TF typologies, higher-risk persons and geographic connections;
b) The typologies, higher-risk persons and geographic connections for which the system monitors are regularly updated.
c) The system is appropriate for and/or sufficiently adjustable to the product or service to which it is to be applied;
d) The system provides the user with the reasons that unusual customer behaviour or a transaction is flagged; and
e) 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 skillsets 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 and conduct that appear to fall outside 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 obligations for RFIs are primarily set forth in Regulations 21 through 31A of POCR. Penalties specific to violations of the abovementioned Regulations are set forth in Regulation 32 of POCR.

8.3 Regulations 21 through 31A are directed toward enhancing the transparency of all transfers of funds, both cross-border and domestic. Specifically, POCR requires 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:

a) RFIs providing transfer services as a payer RFI, intermediary RFI or payee RFI to facilitate the identification and reporting of suspicious transactions; and
b) 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 POCR

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 POCR covers 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 POCR covers international transfers and domestic transfers.

8.7 Despite the broad application of the POCR, several transfer types are exempted in part or whole. Regulation 22 grants specified exemptions for the following:

a) 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 Society for Worldwide Interbank Financial

Telecommunication (SWIFT) and includes MT 400 and MT 700 series messages when they are used to settle trade finance obligations between banks;

b) Transfers by credit card, debit card or pre-paid card, provided that:
   i. The payee has an agreement with the PSP permitting payment for goods or services;
   ii. The transfer is accompanied by a unique identifier permitting the transaction to be traced back to the payer; and
   iii. The card is not used as a payment system to effect a person-to-person transfer of funds;
c) Transfers whereby the payer withdraws cash from their own account. This is designed to exempt ATM withdrawals outside Bermuda that would otherwise require complete information to be included with the transfer;
d) Transfers to public authorities within Bermuda for taxes, fines or other levies;
e) Direct debits, provided they carry a unique identifier for tracing purposes;
f) Truncated cheques (cheques are otherwise paper to which the POCR does not apply);
g) Pre-paid transfers in amounts not exceeding $150 that are carried out by means of a mobile phone or any other digital or Information Technology (IT) device; and
h) 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 an AML/ATF RFI 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:

a) Name;
b) Address; and
c) Account number.

8.10 Complete information on the payee means the payee's:

a) Name; and
b) Account number.

8.11 Where the payer is a natural person, the payer's address may be substituted with the payer's date and place of birth, customer identification number or national identity number.

8.12 Where a payer or payee does not have an account number, the PSP must substitute it

with a unique identifier that allows the transaction to be traced to the payee. See paragraph 8.33.

8.13 PSPs should allow substitutions described in paragraphs 8.11 and 8.12 only to address legitimate business needs and should use the substitutions 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 8.19 to other PSPs involved in the execution of the transfer.

8.14 Where the payer is a legal person, the address should be the address where the company's business is conducted.

8.15 Where the payer is a trust or trustee, the address should be the address of the trustee.

8.16 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.

8.17 Where there is a batch file transfer from a single payer and the payee PSP is situated outside Bermuda, complete information will be considered to have been transferred, provided that:

a) The batch file transfer contains complete information on the payer and each of the payees for each individual transfer;
b) The individual transfers of funds carry the account number of the payer or a unique identifier where an account number is not available; and
c) The complete information provided on all payees is fully traceable within the beneficiary country.

8.18 Account numbers may be, but are not required to be, expressed in International Bank Account Number (IBAN) format.

8.19 Although it is possible that a payee may 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

8.20 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.

8.21 Where any portion of a transfer is cross-border, PSPs should treat all aspects of the transfer as being cross-border.

8.22 Due to the nature of the financial industry in Bermuda, the vast majority of transfers with which Bermudian PSPs are involved are cross-border.

8.23 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 FATF.

8.24 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 is subject to Bermuda disclosure obligations or disclosure obligations equivalent to those in Bermuda.

Obligations on payer PSPs

8.25 Payer PSPs must ensure that each cross-border transfer of funds includes complete information on the payer and payee.

8.26 Where the payer is an accountholder at the payer PSP, the payer PSP must ensure, before transferring funds, that the complete information on the payer conveyed in the payment is accurate and has been verified.

8.27 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 POCR and these GN. Nevertheless, a number of factors may cause a PSP to conduct additional CDD 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 size and nature of the transfer that has been requested in the context of the accountholder's previous transactions and conduct.

8.28 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.

8.29 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.

8.30 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 any altered 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.

8.31 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.

8.32 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 8.31 apply.

8.33 Where the payer or payee is not an accountholder or the transfer is otherwise not drawn from a bank account, the payer or payee PSP, respectively, must produce and include with the transfer a unique identifier that allows the transaction to be traced back to the payer or payee. The POCR 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 or payee. The customer identification number identifies a payer or payee and refers to a record held by the payer or payee PSP, respectively, that contains a customer's name and address, national identity number and/or date and place of birth.

8.34 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 must 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 ensure the prevention of any transfers for which

meaningless or incomplete information has been included in any field.

8.35 Payer PSPs should consider all aspects of ordering and executing a transfer as factors in assessing whether there is knowledge, suspicion or reasonable grounds for suspicion of ML/TF with respect to any transfer of funds or any related transaction. Circumstances that may indicate knowledge, suspicion or reasonable grounds for suspicion of ML/TF include, but are not limited to:

a) A payer who is unwilling or unable to provide the complete information required;
b) A payer for whom the complete information cannot be verified, where it is required to do so;
c) 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;
d) A transfer with missing, meaningless or otherwise incomplete information;
e) A payer seeking to route the transaction through apparently unnecessary intermediary PSPs; and
f) A payer seeking to ensure that the complete information does not reach all PSPs involved in the execution of the payment.

8.36 The payer PSP must keep records for five years of complete information on the payer and payee that accompanies transfers of funds. 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

8.37 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.

8.38 Intermediary PSPs should forward transfers through a messaging system capable of carrying all of the complete information on the payer and payee.

8.39 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:

a) The intermediary PSP informs the payee PSP and any downstream intermediary PSPs of any missing, meaningless or otherwise incomplete information by an agreed form of communication, whether within a messaging service or otherwise;
b) The intermediary PSP keeps a record, for at least five years, of all the information received from the payer PSP or any other intermediary PSP; and

c) Within three working days of receiving any request from the payee PSP, the intermediary PSP makes available to the payee PSP all the information on the payer or payee that the intermediary PSP has received.

8.40 Intermediary PSPs must take reasonable measures commensurate with their risk-based policies, procedures and controls and consistent with straight-through processing to identify transfers of funds that lack complete information for the payer or payee.

8.41 Where an intermediary PSP becomes aware, when receiving a transfer of funds, that information on the payer or payee is incomplete or missing, the intermediary PSP must either:

a) Reject the transfer;
b) Request the complete information on the payer and payee; or
c) Make an internal SAR to the reporting officer.

8.42 An intermediary PSP must also take one or more of the steps outlined in paragraph 8.41 where it knows or suspects that information provided by the payer PSP has been stripped or altered at any point in the payment chain.

8.43 At all times, PSPs must adhere to the acts, regulations and guidance notes addressing tipping-off offences. For more information, see paragraphs 9.82 to 9.88.

8.44 Where a payer PSP or intermediary PSP regularly fails to supply complete information, the intermediary PSP must report that fact to the BMA and must take steps to attempt to ensure that the payer PSP or intermediary PSP provides complete information. Those steps may include:

a) Issuing warnings to the payer PSP or intermediary PSP;
b) Setting deadlines for the payer PSP or intermediary PSP to provide complete information;
c) Rejecting future transfers from the payer PSP or intermediary PSP; or
d) Determining whether to restrict or terminate the business relationship with the payer PSP or intermediary PSP.

8.45 Intermediary PSPs should have risk-based policies, procedures and controls for the following:

a) Identifying transfers, including those carried out with straight-through processing, that lack complete information or include meaningless or otherwise incomplete information;
b) Determining when to execute, reject or suspend such transfers; and
c) Determining appropriate follow-up action with payer PSPs, payee PSPs, other intermediary PSPs and competent authorities.

8.46 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) A transfer with missing, meaningless or otherwise incomplete information;
b) A transfer that has been routed through one or more intermediary PSPs, apparently without a legitimate purpose; and
c) A transfer that appears to have been routed through the intermediary PSP for the purpose of preventing information from reaching the payee PSP.

8.47 Where a PSP controls both the payer and payee side of a transfer of funds, the PSP must:

a) Consider all the information from both the payer and payee sides to determine whether to make a disclosure to the FIA; and
b) Where a decision is made to make a disclosure to the FIA, the PSP must also make a disclosure to the relevant financial intelligence unit in any country affected by the transfer of funds and make relevant transaction information available to the FIA.

8.48 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 pertaining to the payment, including requests for information, whether received through a messaging system or any other means. All records should be kept in accordance with the guidance provided in **Chapter 11: Record-Keeping**.

Obligations on payee PSPs

8.49 Prior to transferring funds, a payee PSP must ensure that the identity of the payee is accurate and verified for any transfer of funds over $1,000 and for any transfer of funds that is carried out in several operations that appear to be linked and together exceed $1,000.

8.50 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 POCR and these GN. Nevertheless, several factors may cause a PSP to conduct additional CDD on an accountholder before 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.

8.51 Where the payee is not an accountholder and the transfer exceeds $1,000, the payee

PSP must 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 payee's identity where a transaction is carried out in several operations that appear to be linked and together exceed $1,000.

8.52 Where the payee is not an accountholder and the transfer is $1,000 or less, the payee PSP must 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 8.51 apply.

8.53 Where the payee is not an accountholder, the payee PSP must 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 8.33.

8.54 Payee PSPs must have effective policies, procedures and controls, including post-event monitoring or real-time monitoring where feasible, to detect whether incoming transfers of funds include all required information.

8.55 In practice, some messaging systems will not allow a transfer to reach a payee PSP without each required field being populated. Payee PSPs must have risk-based policies, procedures and controls to identify transfers for which meaningless or incomplete information has been included in any field.

8.56 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:

a) Reject the transfer;
b) Request the complete information on the payer and payee; or
c) Make an internal SAR to the reporting officer.

8.57 A payee PSP should also take one or more of the steps outlined in paragraph 8.56 where it knows or suspects that information provided by the payer PSP or any intermediary PSP has been stripped or altered at any point in the payment chain.

8.58 At all times, PSPs must adhere to the acts, regulations and guidance notes addressing tipping-off offences. For more information, see paragraphs 9.82 through 9.88.

8.59 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.

8.60 Where, despite the payee PSP taking the steps described in paragraph 8.59, a payer PSP still regularly fails to provide all required information on the payer and payee, the payee PSP must either reject any future transfers of funds from the payer PSP or determine whether to restrict or terminate the business relationship with the payer PSP, either completely or in respect of funds transfers.

8.61 Payee PSPs should also apply paragraphs 8.59 through 8.60 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.

8.62 Where real-time monitoring is not feasible, payee PSPs must conduct post-event monitoring through the use of risk-based sampling to determine whether complete information on the payer and payee is included with each transfer. Such sampling may include but is not limited to:

a) Cross-border transfers of funds as defined in paragraph 8.20;
b) Transfers involving higher-risk customers and jurisdictions, as identified by the PSP's risk assessment processes;
c) Transfers involving multiple intermediaries;
d) Transfers involving payer PSPs or intermediary PSPs that have previously failed to provide all required information;
e) Transfers involving PSPs known via reliable sources to have stripped or altered information provided by the payer PSP;
f) Transfers for which alternative information has been substituted for the payer's address;
g) Transfers above the $1,000 threshold to non-accountholders; and
h) Transfer chains involving two or more PSPs that are bound by different sanctions regimes.

8.63 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 or that there are reasonable grounds to be suspicious include but are not limited to:

a) A transfer with missing, meaningless or otherwise incomplete information;
b) A transfer that has been routed through one or more intermediary PSPs, apparently without a legitimate purpose;
c) 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
d) A transfer for which there is evidence to suggest that a person other than the named payee is the intended final recipient.

8.64 Where a PSP controls both the payer and payee side of a cross-border transfer of funds, the PSP must:

a) Consider all the information from both the payer and payee sides to determine whether to make a disclosure to the FIA; and
b) Where a decision is made to make a disclosure to the FIA, the PSP must also make a disclosure to the relevant financial intelligence unit in any country affected by the transfer of funds and make relevant transaction information available to the FIA.

8.65 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.

8.66 The payee PSP must maintain records of all information received from the payer PSP and any intermediary PSPs for at least five years. 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

8.67 Under Regulation 25 of POCR, where there is a batch file transfer from a single payer and the payees' PSP is situated outside Bermuda, complete information will be considered to have been transferred, provided that:

a) The batch file transfer contains complete information on the payer and each of the payees for each individual transfer;
b) The individual transfers of funds carry the account number of the payer or a unique identifier where an account number is not available; and
c) The complete information provided on all payees is fully traceable within the beneficiary country.

Domestic transfers of funds

8.68 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.

8.69 The payer PSP must provide the payee PSP or any competent authority with the complete information on the payer within three working days of receiving any request from the payee PSP or competent authority, respectively.

Money or value transfer service providers

8.70 Money or value transfer service providers are required to comply with the acts, regulations and guidance notes addressing wire transfers.

8.71 Where a money or value transfer service provider PSP controls both the payer and payee sides of a cross-border transfer of funds, the PSP must:

a) Consider all the information from both the payer and payee sides to determine whether to make a disclosure to the FIA; and
b) Where a decision is made to make a disclosure to the FIA, the PSP must also make a disclosure to the relevant financial intelligence unit in any country affected by the transfer of funds and make relevant transaction information available to the FIA.

Minimum standards

8.72 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 complete information.

8.73 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, Sections 5 through 12 of ATFA and Regulations 16 and 17 of POCR.

9.3 The phrase 'suspicious activity' refers to any transaction, act or conduct that results in an RFI's employee having knowledge, suspicion or reasonable grounds for suspicion that funds or assets are criminal property or that a person is involved in ML/TF.

9.4 RFIs must put in place appropriate policies and procedures to ensure suspicious activity is identified, enquired into, documented and reported.

9.5 An RFI's policies and procedures for suspicious activity reporting must ensure that:

a) The RFI's employees are trained to identify and report suspicious activity related to criminal property and ML/TF;
b) The RFI's employees provide an internal SAR to the reporting officer where there is knowledge, suspicion or reasonable grounds for suspicion that funds or assets are criminal property or that a person is involved in ML/TF;
c) The RFI's reporting officer considers all internal SARs in light of all relevant and available information and requires appropriate enquiries to be made;
d) The RFI's reporting officer promptly reports to the FIA as soon as is practicable where the reporting officer finds that the SAR reported internally, in light of all relevant and available information, evidential knowledge, suspicion or reasonable grounds for suspicion that funds or assets are criminal property, or that a person is involved in ML/TF;
e) The RFI does not make any funds available to any person specified by written notice received from the FIA for a period not exceeding 72 hours; and
f) The RFI's employees understand that it is a criminal offence to disclose to any person other than the reporting officer or the FIA any knowledge, suspicion or reasonable grounds for suspicion that a disclosure has been filed with the FIA or any other information or other matter likely to prejudice any investigation, which might be conducted following such a disclosure.

9.6 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 promptly make an external report to the FIA where

there is knowledge, suspicion or reasonable grounds for suspicion that funds or assets are criminal property or that a person is involved in ML/TF.

What is meant by 'knowledge' and 'suspicion'?

Knowledge

9.7 Having knowledge means knowing the existence of certain facts. In a criminal court, to have knowledge, it must be proved that the natural person, in fact, knew that funds or assets were criminal property or that a person was engaged in ML/TF.

9.8 Nevertheless, 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.

9.9 Section 46 of POCA and Schedule 1 of ATFA 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

9.10 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."

Reasonable grounds to suspect

9.11 Reasonable grounds to suspect is a purely objective standard. Reasonable grounds to suspect does not require any person to actually form suspicion. Instead, reasonable grounds to suspect arises when a reasonable person would form suspicion based on the information available at the time.

9.12 Guidance regarding the establishment of norms for transactions or activities and the identification of unusual transactions or conduct that fall outside of those established norms, is provided in paragraphs 7.11 through 7.14.

9.13 A transaction or conduct that appears unusual does not necessarily create suspicion or reasonable grounds for suspicion. 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 or provide reasonable grounds for suspicion but should cause the RFI to conduct further, objective enquiries to determine whether or not the transaction or conduct is indeed suspicious or provides

reasonable grounds for suspicion.

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 and Section 10A of ATFA. For further guidance, see paragraphs 9.82 through 9.88.

9.16 Where an employee conducts enquiries regarding an unusual transaction or unusual conduct and obtains what a reasonable person in similar circumstances would consider to be a satisfactory explanation of the transaction or conduct, they may conclude that there are no reasonable grounds for suspicion, and they may conclude the enquiries by making a record of their findings. Nevertheless, where the employee's enquiries do not provide a satisfactory explanation of the transaction or conduct, they must conclude that there are reasonable grounds for suspicion and must make an internal report.

9.17 A report of each enquiry made in respect of an unusual transaction or unusual conduct should be documented or recorded electronically and retained in accordance with the guidance provided in **Chapter 11: Record-Keeping**.

9.18 A transaction or conduct may not be suspicious at the time it takes place, but suspicions or reasonable grounds for suspicion that arise at a later time must nonetheless be reported. Where an intended transaction or intended conduct appears suspicious or provides reasonable grounds for suspicion (whether or not it ultimately took place), an internal report should be made before the transaction or conduct occurs. Where a transaction or conduct appears suspicious or provides reasonable grounds for suspicion only in hindsight, an internal report must be made after the transaction or conduct has been completed.

9.19 Internal reports that are made after the transaction or conduct 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, the offence of ML 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 that 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, the duty to report applies in relation to any TF offence

under Sections 5 through 8 of ATFA that a person is committing, attempting to commit or has committed, which would have been an offence under these sections of ATFA 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, suspicion or reasonable grounds for suspicion that funds or assets are the criminal property or that a person is involved in ML/TF.

9.23 Internal SARs to the reporting officer must be made promptly.

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, suspicion or reasonable grounds for 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 or whether there are reasonable grounds for suspicion, 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; they must not allow any colleague to decide for them.

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: Record-Keeping**.

9.30 Each internal report should include full details of the customer, transaction, act or conduct in question and as full a statement as possible of the information or conduct giving rise to the knowledge, suspicion or reasonable grounds for suspicion.

9.31 Where a Bermuda RFI is performing outsourcing functions for an institution outside of Bermuda and an external SAR is to be filed outside of Bermuda, the Bermuda RFI must also submit an external SAR to the FIA in Bermuda. See paragraphs 9.49 and 9.87.

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, suspicion or reasonable grounds for suspicion, an internal report must be made to the Bermuda RFI's reporting officer.

9.33 Once an employee has reported their suspicion in an appropriate manner to the reporting officer or to a natural person to whom the reporting officer has delegated the responsibility to receive such internal reports, the reporting employee has fully satisfied their 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 SARs and to determine whether an external SAR 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, suspicion or reasonable grounds for suspicion that funds or assets are criminal property or that a person is involved in ML/TF.

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 FIA.

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 5.131 through 5.140 and 5.167 through 5.168.

9.39 Additional relevant information may include that which arises:

a) Commercially, through linked accounts, third-party service providers and introducers;
b) Individually, through persons such as third parties, beneficial owners, controllers or signatories; or
c) Through other means, including publicly 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 and Section 10A of ATFA. For further guidance, see paragraphs 9.82 through 9.88.

9.41 When evaluating an internal report, the reporting officer taking account of the risk posed by the transaction or conduct in question should strike the appropriate balance between the requirement to make prompt disclosure to the FIA 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 FIA prior to completing a full review of the business relationship and any linked or connected relationships. Any initial report must be followed promptly by a full SAR. For additional information, see paragraph 9.52.

9.43 If the reporting officer determines that a report to the FIA is not appropriate, the reasons for the determination should be clearly documented and retained in accordance with the guidance provided in **Chapter 11: Record-Keeping**.

External suspicious activity reporting

9.44 Where, after evaluating an internal SAR, the reporting officer determines that there is knowledge, suspicion or reasonable grounds for suspicion that funds or assets are criminal property or that a person is involved in ML/TF, the reporting officer must promptly file an external SAR with the FIA.

9.45 RFIs should include in each external SAR as much relevant information about the customer, transaction, counterparty or activity as it has in its records.

9.46 Each external SAR must be made promptly after the information comes to the attention of the reporting officer.

9.47 Each external SAR to the FIA should be documented and retained in accordance with the guidance provided in **Chapter 11: Record-Keeping**.

9.48 For all AML/ATF matters, contact between particular departments or branches of an RFI and the FIA 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, it may be appropriate to route communications through an appropriate employee in the RFI's legal or compliance department.

9.49 Within a financial group, where a Bermuda RFI's internal SAR 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 SAR to the FIA.

Where to report

9.50 To avoid committing a failure to report the offence, reporting officers must make their external reports to the FIA, which is the central point for reporting knowledge, suspicion and reasonable grounds for suspicion and, where appropriate, for providing consent to proceed with the transaction or conduct.

9.51 As of October 2011, the FIA no longer accepts any manually submitted SARs (including those faxed or emailed). The FIA accepts only those SARs 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 FIA may be made by telephone but must be followed up promptly by a full SAR.

9.53 The FIA is located on the 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, suspicion or reasonable grounds for suspicion

9.54 Section 46 of POCA and Schedule 1 of ATFA require RFIs to report any knowledge, suspicion or reasonable grounds for suspicion that:

a) Currency, funds or other assets are derived from or used in connection with any criminal conduct;
b) An ML offence has been committed, is in the course of being committed or has been attempted; or
c) Another person is committing, attempting to commit or has committed a TF offence.

9.55 Such reports should be made regardless of whether any attempted activity actually occurs.

Penalties

9.56 Where an employee fails to comply with the obligations under Section 46 of POCA or Schedule 1 of ATFA to make disclosures to a reporting officer and/or to the FIA promptly after information giving rise to knowledge, suspicion or reasonable grounds for suspicion comes to the attention of the employee, the employee is liable to criminal prosecution.

9.57 The criminal sanction, under POCA and ATFA, 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.

9.58 Sections 20A through 20I of POCA SEA grant the BMA other enforcement powers when it considers that an RFI has contravened a requirement imposed on it, including the requirement to report suspicious activity. Those other enforcement powers include the following powers to:

a) Issue directives;
b) Restrict an RFI's licence;
c) Revoke an RFI's licence;
d) Publicly censure a person;
e) Prohibit a natural person from performing functions in relation to an AML/ATF regulated activity; and
f) Wind up or dissolve a company or firm that is or has been a licensed entity.

9.59 Section 20H of POCA SEA grants the court the authority to enter an injunction where there is a reasonable likelihood that any person will contravene a requirement under POCR or any direction or licence condition imposed by the BMA.

FIA response and consent

9.60 External reports to the FIA that are made through the goAML system will be immediately acknowledged.

9.61 Under Article 15 of the Financial Intelligence Agency Act 2007, the FIA 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, not including any Saturday or public holiday.

Consent

9.62 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 FIA.

9.63 The FIA may provide consent. Under Section 44 of POCA and Section 12 of ATFA, a person does not commit a ML/TF offence if, prior to carrying out the transaction or activity, they make an external report to the FIA and later carries out the transaction or activity with the express consent of the FIA.

9.64 RFIs may also regard as having received consent from the FIA if they do not receive notice of refusal from the FIA within seven working days following the day a disclosure is made and where the moratorium period of 45 days has expired. Nevertheless, RFIs should contact the FIA 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 of the transaction or activity. Any guidance provided by the FIA does not constitute legal advice.

9.65 Where a transaction or activity giving rise to knowledge, suspicion or reasonable grounds for suspicion of ML/TF 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 their attention), and on their own initiative, they make an external report promptly. This principle applies equally to an employee of an RFI who makes an internal report to the reporting officer about knowledge, suspicion or reasonable grounds for suspicion, in accordance with the RFI's policies, procedures and controls, provided that the report is made promptly on their own initiative.

9.66 Consent only applies where there is prior notice to the FIA of the transaction or activity. The FIA cannot provide consent after the transaction or activity has occurred.

Requests for additional information

9.67 Under Article 16 of the Financial Intelligence Agency Act 2007, the FIA may, in the course of enquiring into a suspicious transaction or activity relating to ML/TF, serve a notice in writing on any person requiring the person to provide the FIA with such information as it may reasonably require for the purpose of its enquiry.

9.68 A person who is required to provide information must provide the information to the FIA in such a manner as the FIA requires.

9.69 To the extent possible, the FIA 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

9.70 RFIs should maintain one or more registries containing record of the following:

a) Reports of all enquiries made in respect of unusual transactions;
b) All internal reports made to the reporting officer;
c) Reports of all enquiries made in respect of internal reports;
d) The reasons why any internal report was not reported externally to the FIA;
e) All external reports made to the FIA; and
f) All communications, enquiries, notices, directions and expressions of consent from the FIA related to external reports made to the FIA.

9.71 Each registry should include:

a) The date of the report;
b) The name of the person who made the report;
c) The names of any person who added comments to the report;

d) The name of the recipient of the report; and
e) A reference by which all related and supporting documentation may be identified and located.

9.72 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 or reasonable grounds for suspicion are either confirmed or disproved.

9.73 The records in the registry or registries must be retained in accordance with the guidance provided in **Chapter 11: Record-Keeping**.

Transactions following a disclosure

9.74 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, suspicion or reasonable grounds for suspicion that the additional transaction or activity involves criminal property or that a person is involved in ML/TF.

Declining or terminating business

9.75 It is normal practice for RFIs to turn away proposed business that they know, suspect or have reasonable grounds to suspect might be criminal in intent or origin. In such circumstances, RFIs must also make an external report to the FIA, regardless of whether a transaction or activity has taken place.

9.76 RFIs should refrain from referring such declined business to other institutions.

9.77 Whether to establish or terminate a business relationship is generally a commercial decision. At times, however, the refusal or termination of a business relationship may be required by act or regulation, for example, under Regulation 9 of POCR where an RFI is unable to apply CDD measures in accordance with the POCR.

9.78 The consent of the FIA for an RFI to carry out a transaction or activity is not intended to override normal commercial judgement. Consent from the FIA provides a defence against a charge of committing a ML/TF offence under Sections 44 and 45 of POCA and Sections 5 through 8 of ATFA. Consent on its own does not create an obligation to continue a relationship.

9.79 Where an RFI decides to terminate a relationship after making an external report to the FIA 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 FIA.

9.80 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 FIA before returning the funds.

9.81 The practices described in paragraphs 9.75 through 9.80 above are consistent with international best practices.

Tipping-off

9.82 Section 47 of POCA and Section 10 of ATFA contain tipping-off offences.

9.83 It is an offence if a person knows, suspects or has reasonable grounds to suspect that an internal or external report has been made to the reporting officer or the FIA, and the person discloses to any other person:

a) Knowledge or suspicion that a report has been made; and/or
b) Any information or other matter likely to prejudice any investigation which might be conducted following such disclosure.

9.84 It is also an offence if a person knows, suspects or has reasonable grounds to suspect that a police officer is acting or proposing to act in connection with an actual or proposed investigation of ML/TF and the person discloses to any other personal information or any other matter likely to prejudice the actual or proposed investigation.

9.85 Reasonable enquiries of a customer regarding the background and purpose of a transaction or activity that has given rise to suspicion or reasonable grounds for suspicion form an integral part of CDD and ongoing monitoring. Where such enquiries are conducted in a manner that does not indicate any knowledge or suspicion of ML/TF, they should not give rise to tipping-off.

9.86 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 FIA. Any guidance provided by the FIA does not constitute legal advice.

9.87 Where one member or office of a financial group has made or will make an external report to the FIA, that fact may be disclosed to another member or office of the same financial group provided that:

a) The disclosure is for the purposes of discharging AML/ATF responsibilities and functions; and
b) There are no grounds to believe the disclosure may prejudice an actual or proposed investigation.

9.88 RFIs may wish to seek legal advice to determine whether the criteria set forth in paragraph 9.87 are fulfilled.

Constructive trusts

9.89 An RFI holding funds or assets that it knows, suspects or has reason to suspect 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.

9.90 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.

9.91 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.

9.92 Where an RFI has the suspicion or reasonable grounds for suspicion it considers necessary to report under the AML/ATF acts and regulations, the suspicion or reasonable grounds for suspicion, in certain circumstances, may indicate that the RFI:

a) Knows that the funds or assets do not belong to its customer; or
b) Is on notice that the funds or assets may not belong to its customer.

9.93 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.

9.94 If, when making an SAR, 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 FIA.

9.95 If the customer wishes subsequently to withdraw or transfer the funds or assets, the RFI should, in the first instance, contact the FIA for guidance.

9.96 Any consent that the FIA 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.

9.97 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.

9.98 The effective application of the CDD and ongoing 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

9.99 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 FSIU. These obligations are explained in greater detail in **Chapter 6: International Sanctions**.

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 of POCR. The criminalisation of involvement with ML/TF and the requirement that employees report knowledge, suspicion or reasonable grounds for suspicion of ML/TF are set forth in Sections 43 through 46 of POCA and Sections 6 through 8 and Schedule 1 Part 1 of ATFA. The tipping-off offences relevant to an RFI's employees are set forth in Section 47 of POCA and Section 10A of ATFA.

10.3 RFIs must take appropriate measures to ensure that relevant employees:

a) Are aware of the acts and regulations relating to ML/TF;
b) Undergo training on how to identify transactions which may be related to ML/TF; and
c) 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:

a) Risk assessment and management;
b) CDD measures;
c) Ongoing monitoring;
d) Record-keeping;
e) Internal control; and
f) International sanctions (see paragraphs 6.52 through 6.54).

10.5 An RFI's training programme should be ongoing 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 GN, the term employee includes any person working for an RFI, including senior management, members of the governing body and other persons working under a contract of employment or under a contract for services. A relevant employee is one who:

a) At any time in the course of their duties, has or may have access to any information that may be relevant in determining whether funds or assets are criminal property, or that a person is involved in ML/TF; or
b) At any time, plays a role in implementing and monitoring compliance with AML/ATF requirements.

10.7 Temporary employees carrying out activities in section 10.6, sub-paragraph a or b must also receive appropriate training.

10.8 Where employees of any Bermuda-based third parties carry out activities in section 10.6, subparagraph a or b 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 1.59 through 1.72.

Legal obligations on employees

10.10 Several offences under POCA and ATFA directly affect the employees of an RFI:

a) The various offences of ML/TF (see paragraph 1.24);
b) Failure to report knowledge, suspicion or reasonable grounds for suspicion of ML/TF (see paragraphs 9.56 through 9.59); and
c) Tipping-off and disclosure of information (see paragraphs 9.82 through 9.88).

10.11 These offences 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 ongoing training on the acts, 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 perform their job functions properly.

10.15 The training programme 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:

a) The acts, regulations and guidance notes relating to ML/TF;
b) The acts, regulations and guidance notes relating to PEPs (see paragraphs 5.96 through 5.116) and **Annex IV: Risk Factors for PEPs**;
c) The acts, regulations and guidance notes relating to international sanctions (see **Chapter 6: International Sanctions**, in particular, paragraphs 6.52 through 6.54);
d) The employee's responsibilities under the RFI's AML/ATF policies, procedures and controls;
e) The ML/TF threats the business faces;
f) The vulnerabilities of the RFI's products, services, delivery channels, transactions and business relationships;
g) The consequences to the RFI, its employees personally and its clients due to a breach of the acts, regulations or guidance notes relating to ML/TF;
h) How to identify transactions which may be related to ML/TF;
i) The identity and responsibilities of the reporting officer; and
j) How to properly report suspicions and reasonable grounds for suspicion 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, delivery channels, transactions and business relationships. 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, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services,

delivery channels, products and transactions. For additional information, see paragraphs 2.62 through 2.68.

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 (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and 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 ongoing monitoring, see **Chapter 7: Ongoing Monitoring**.

10.22 RFIs must train relevant employees to recognise unusual or suspicious transactions or conduct and to properly report knowledge, suspicion and reasonable grounds for suspicion of ML/TF.

10.23 The circumstances giving rise to unusual transactions or conduct and which may give rise to knowledge, suspicion or reasonable grounds for suspicion of ML/TF, depend on the specific combination of customers, business relationships (including outsourcing and reliance relationships), countries or geographic areas, services, delivery channels, products and transactions 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, suspicion or reasonable grounds for suspicion of ML/TF:

a) Transactions which have no apparent purpose, which make no obvious economic sense or which involve apparently unnecessary complexity;
b) The use of non-resident accounts, companies or structures in circumstances where the customer's needs do not appear to support such economic requirements;
c) 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;
d) Dealing with customers not normally expected in that part of the business;
e) Transfers to and from high-risk jurisdictions, without reasonable explanation, which are not consistent with the customer's declared foreign business dealings or interests;
f) A transaction that is structured just below the 'occasional transaction' threshold to avoid CDD requirements;

g) 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;
h) Unnecessarily routing funds through third-party accounts; and
i) 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) A customer who refuses or appears particularly reluctant to provide the information requested without reasonable explanation;
b) A customer who is unable or unwilling to explain a client entity's legal and corporate structure, ownership or control;
c) A customer who provides information that is inconsistent or in conflict with other information the RFI holds;
d) 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;
e) A customer who opens an account or relationship in a jurisdiction that appears inconsistent with the customer's known business;
f) A customer with other business relationships with the RFI and for whom customer information, transactions or conduct are inconsistent across the different relationships;
g) A customer who wants to conclude arrangements with unusual urgency against an unsatisfactorily explained promise to provide information at a later stage; and
h) 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. Nevertheless, 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, ongoing 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 of POCR.

11.3 Record-keeping is an essential component of establishing an audit trail. Proper record-keeping enables AML/ATF processes to keep criminal property out of the financial system and, when required, detect criminal property and ensure its 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 the reconstruction of individual transactions so as to provide, where necessary, evidence for the prosecution of criminal activity.

11.5 To comply with the POCR Regulations and these GN, the records an RFI keeps should be such that:

a) The RFI's managers and auditors will be able to assess the effectiveness of the RFI's AML/ATF policies and procedures;
b) Any transactions or instructions effected via the RFI on behalf of any particular customer can be reconstructed;
c) The audit trail for funds entering and leaving Bermuda is clear and complete;
d) Any customer can be properly identified and located;
e) A customer profile can be established for all customers for whom there is a business relationship;
f) All suspicions identified internally and all SARs made externally can be understood; and
g) The RFI can satisfy, within the time frames set out in the regulations, any authorised information requests or court orders from the appropriate authorities.

Specified records to retain

<u>CDD</u>

11.6 RFIs must retain all records obtained in the course of conducting CDD. Such records include those obtained during the application of both initial and ongoing

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.

11.7 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.

11.8 Where CDD is applied using online or other electronic databases, RFIs, either themselves or through third parties, which the RFI has confirmed as meeting the retrieval of records requirements in paragraphs 11.18 through 11.22, must retain a record of the means by which each verification was completed and, where applicable, the data supporting each verification.

11.9 To ensure that the objectives of paragraph 11.5 are met, RFIs should maintain records concerning:

a) Data obtained through the application of CDD measures;
b) Copies or records of official identification documents;
c) Customer verification documents;
d) Customer-related data obtained from any reliable and independent source;
e) Information obtained during a customer visit to an RFI's agent or premises;
f) Information obtained for the purposes of enhanced CDD or ongoing monitoring;
g) Verification information as to beneficial ownership;
h) Information concerning the nature of the business and the purpose and intended nature of the business relationship; and
i) Account files and correspondence.

<u>Transactions</u>

11.10 RFIs must retain supporting records of transactions consisting of the original documents or copies admissible in court proceedings. The supporting records must be sufficient to permit the reconstruction of individual transactions. To satisfy these requirements, transaction records should be kept of the following:

a) The volume of funds flowing through the account;
b) The origin of the funds;
c) The form (e.g., cheque, wire transfer) and currency in which the funds were received or withdrawn;
d) The identity of the person undertaking the transaction;
e) The name and address (or identification code) of the counterparty;
f) The destination of the funds;
g) The form of instruction and authority;
h) Whether the transaction was a purchase or a sale;

i) 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);
j) Any security dealt in, including price and size;
k) Any original vouchers not returned to the customer or the customer's agent; and
l) Any large item/exception reports created in the course of transaction monitoring.

Timing

11.11 RFIs must keep CDD information (see paragraphs 11.6 through 11.9) for the duration of a business relationship and for at least five years beginning on the date on which the business relationship ends. In the case of an occasional transaction, RFIs must keep CDD information for at least five years, beginning on the date on which the transaction is completed.

11.12 RFIs must keep transaction information (see paragraph 11.10) for at least five years, beginning on the date the transaction is completed.

11.13 Where an SAR is made to the FIA, 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.

11.14 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.

11.15 An RFI must establish and maintain policies, procedures and controls that enable it to respond fully and rapidly to enquiries received from the FIA or law enforcement relating to:

a) Whether it maintains or has maintained during the previous five years a business relationship with any person; and
b) The nature of that relationship.

Other Records

<u>Training</u>

11.16 With respect to AML/ATF training, an RFI's records should include:

a) Dates AML/ATF training was given;
b) The nature of the training;
c) The name(s) of the person(s) giving the training;
d) The names of the employees who received training; and
e) The results of the tests undertaken by employees, where appropriate.

Internal and external reports

11.17 With respect to internal and external reports, an RFI's records should include:

a) The results of any account or transaction-related analysis;
b) Reports by the compliance officer to senior management;
c) Records of consideration of internal compliance reports and actions taken as a consequence;
d) Where no SAR was made to the FIA, records of the material that was considered and the basis for determining that no SAR was required;
e) Copies of any SAR made to the FIA; and
f) ML/TF enquiries from the authorities.

Retrieval of records

11.18 Regardless of whether a transaction was undertaken by paper or electronic means, the record retention requirements are the same.

11.19 Records, including copies of original documents, may be kept in hard copy or electronic format, provided that RFIs can retrieve them without delay.

11.20 Where records, whether in physical or electronic form, are held outside of Bermuda or by any third party, 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.

11.21 An RFI must not rely on a person or enter into any outsourcing arrangement where access to the records without delay is likely to be impeded by confidentiality or data protection restrictions. 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.

11.22 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 backup form, RFIs should ensure that policies, procedures and controls are in place to detect promptly any data breach.

Third parties and financial groups

11.23 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 POCR and these GN.

11.24 During the termination of a third-party reliance situation or an outsourcing arrangement, an RFI should ensure that it obtains and retains all appropriate records

or oversees their transfer to another designated third party.

11.25 Where one member of a financial group ceases to trade or have a business relationship with a customer and where the customer relationship continues with other members of the financial 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 group.

11.26 Where relevant records are held by one member of a financial 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 access the information immediately and retrieve copies of the records without delay.

11.27 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

All sector-specific guidance notes are being updated under separate cover and will be provided for consultation with industry in due course.

ANNEX II: SECTOR-SPECIFIC GUIDANCE NOTES FOR INSURANCE BUSINESS

All sector-specific guidance notes are being updated under separate cover and will be provided for consultation with industry in due course.

ANNEX III: SECTOR-SPECIFIC GUIDANCE NOTES FOR SECURITIES SECTOR

All sector-specific guidance notes are being updated under separate cover and will be provided for consultation with industry in due course.

ANNEX IV: RISK FACTORS FOR PEPS

IV.1 This annex contains a non-exhaustive list of risk factors relating to PEPs.

Risk factors relating to a PEP's attempt to shield their 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:

a) Legal entities and legal arrangements to obscure the beneficial owner;
b) Legal entities and legal arrangements without a valid business reason;
c) 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
d) 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:

a) The use of legal entities and legal arrangements to obscure ownership or the involvement of a particular person, industry or jurisdiction;
b) A PEP inquiring about an RFI's AML/ATF or PEP policies, procedures or controls;
c) A PEP who is unable or reluctant to provide information establishing the source of wealth or source of funds;
d) Information provided by a PEP that is inconsistent with publicly available information, such as asset declarations or published official salaries;
e) A PEP who is unable or reluctant to explain the reason for doing business in the jurisdiction of the RFI;
f) A PEP who provides inaccurate or incomplete information;
g) A PEP who seeks services from an RFI that would normally not cater to foreign or high-value clients;
h) The repeated transfer of funds to and from jurisdictions with which the PEP does not appear to have ties;
i) A PEP who has been denied a visa or entry to the country or territory; and
j) 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 their position are important factors to be taken into account. Possible risk factors include:

a) A PEP with access to or authority over state funds, assets, policies or operations;
b) A PEP with control over regulatory approvals, including the awarding of licences and concessions;
c) A PEP with the formal or informal ability to control mechanisms established to prevent or detect ML/TF;
d) A PEP who actively downplays the importance of their public function;
e) A PEP who does not provide all their titles or positions, including those that are *ex officio*;
f) A PEP with access to, or control or influence over, government or corporate accounts;
g) A Pep who controls, in part or in whole, any financial institution or Designated Non-Financial Business and Professions, either privately or *ex officio*; and
h) 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

V.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:

a) Arms trade and defence industry;
b) Banking and finance;
c) Business active in government procurement (e.g., those whose business is selling to government or state agencies);
d) Construction and major infrastructure;
e) Development and other types of assistance;
f) Human health activities;
g) Mining and extraction;
h) Privatisation; and
i) Provision of public goods, including utilities.

Risk factors relating to a business relationship or transaction

VI.6 Risk factors may relate to a specific business relationship or transaction. Examples of such risk factors include:

a) The submission of multiple suspicious transaction reports with regard to a PEP or a business relationship involving a PEP;
b) The consistent use of rounded transaction amounts, where such use falls outside of the norm for the expected business;
c) Large deposits or withdrawals into or from an account, using cash, bank cheques or other bearer instruments;

d) Another RFI's termination of a business relationship with a PEP;
e) Another RFI's exposure to regulatory action due to a business relationship with a PEP;
f) Difficulty distinguishing between a person's personal and business money flows;
g) Financial activity that is inconsistent with legitimate or expected activity;
h) The movement of funds into or out of an account or between financial institutions without a business rationale;
i) An account with unexpected and/or substantial activity after a dormant period, over a relatively short period, or shortly after commencing a business relationship;
j) An account featuring unusual cash or wire transfer transactions;
k) Transactions between non-client corporate vehicles and the PEP's account(s);
l) A PEP who is unable or reluctant to provide details and credible reasons for establishing a business relationship or conducting a transaction;
m) 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;
n) A PEP who uses third parties to exchange gaming chips for cash and vice versa with little or minimal gaming activity; and
o) A PEP who uses multiple bank accounts with no apparent commercial or other legitimate reason.

<u>Products, services, transactions and delivery channels</u>

IV.7 Examples of products, services, transactions and delivery channels, which are of a higher risk, include:

a) Private banking;
b) Anonymous transactions, including cash and NPMs;
c) Non-face-to-face business relationships or transactions;
d) Payments received from unknown or un-associated third parties;
e) Businesses that cater mainly to high-value foreign clients;
f) Trust and company service providers;
g) Wire transfers to and from a PEP's account that cannot be economically explained or that lack relevant originator or beneficiary information;
h) Correspondent and concentration accounts;
i) Dealers in precious metals and precious stones or other luxurious goods;
j) Dealers in luxurious transport vehicles, such as cars, sports cars, ships, helicopters and planes; and
k) 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) A foreign or domestic PEP from a high-risk jurisdiction, particularly where the PEP has control or influence over decisions affecting the jurisdiction's AML/ATF system;
b) Foreign or domestic PEPs from a jurisdiction identified by credible sources as having a higher risk of corruption;
c) 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 Organisation for Economic Co-operation and Development Anti-Bribery Convention;
d) 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;
e) Foreign or domestic PEPs from a jurisdiction that is dependent on the export of illicit goods, such as drugs;
f) 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;
g) Foreign or domestic PEPs from a jurisdiction with poor and/or opaque governance and accountability; and
h) 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:

a) Monitoring AML/ATF RFIs to ensure full compliance with Bermuda's AML/ATF framework;
b) Assisting with the detection and prevention of financial crime;
c) Deterring criminal and terrorist activity by increasing the risk that perpetrators will be detected and by lowering the reward that perpetrators receive; and
d) Issuing guidance to AML/ATF RFIs supervised for compliance with the AML/ATF regulations.

V.2 Bermuda Police Service

Bermuda's law enforcement body responsible for detection, investigation and public education to promote public safety and crime prevention for all criminal activity in Bermuda, which includes ML, acts of terrorism and TF.

V.3 Financial Intelligence Agency

Bermuda's FIA is the recipient of financial information from various sources, most notably SARs, which allows them to analyse and develop financial intelligence to support law enforcement, supervisors, foreign FIA counterparts, as well as industry to effectively carry out their various functions.

V.4 HM Customs

Bermuda's first line of defence in border control, which is responsible for:

a) Interdicting illicit drugs and contraband;
b) Monitoring the movement of passengers and cargo;
c) Monitoring cash declarations on export or import;
d) Monitoring the cross-border movements of currency and bearer negotiable instruments; and
e) Enforcing compliance with Bermuda's customs laws and regulations.

V.5 National Anti-Money Laundering Committee

A Bermudian inter-governmental committee, which was established under Section 49 of POCA for the purpose of:

a) Advising the Minister of Finance in relation to the detection and prevention of ML 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 ML, and;

b) Advising the Minister of Finance as to the participation of Bermuda in the international effort against ML.

The Chairman of the Committee is appointed by the Minister of Finance and must be a person with relevant experience. The Committee meets on a regular basis to carry out its duties. The statuatory members of the Committee are:

a) Chairman;
b) Solicitor General;
c) Financial Secretary;
d) Commissioner of Police;
e) Director of the FIA;
f) Chief Executive Officer of the BMA;
g) Director of Public Prosecutions;
h) Permanent Secretary Ministry of Legal Affairs and Constitutional Reform;
i) Collector of Customs;
j) National Coordinator;
k) Registrar General;
l) Registrar of Companies (including when acting in their capacity as Superintendent of Real Estate); or
m) Such other persons as the Minister of Finance 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 ML/TF.

V.7 Superintendent of Real Estate

Bermuda's supervisory authority in relation to relevant persons that are real estate brokers or real estate agents.

V.8 Barristers and Accountants AML/ATF Board

Bermuda's supervisory authority for relevant persons that are regulated professional firms of barristers or accountants who carry out 'specified activities' as defined in section 49(5) of POCA.

V.9 Bermuda Casino Gaming Commission

Bermuda's supervisory authority for relevant persons that are casino operators.

ANNEX VI: CORPORATE SERVICE PROVIDER BUSINESS

All sector-specific guidance notes are being updated under separate cover and will be provided for consultation with industry in due course.

ANNEX VII: MONEY SERVICE BUSINESS

All sector-specific guidance notes are being updated under separate cover and will be provided for consultation with industry in due course.

ANNEX VIII: DIGITAL ASSET BUSINESS

All sector-specific guidance notes are being updated under separate cover and will be provided for consultation with industry in due course.