Annex VII

Sector-Specific Guidance Notes for Money Service Business

These Sector-Specific Guidance Notes (SSGN) are annexed to, and should be read in conjunction with, the Guidance Notes for Anti-Money Laundering/Anti-Terrorist Financing (AML/ATF) Regulated Financial Institutions on AML/ATF 2022 (GN)

Table of Contents

ANNEX VII

SECTOR-SPECIFIC GUIDANCE NOTES FOR MONEY SERVICE BUSINESS

Introduction

VII.1 This annex sets forth guidance on AML/ATF obligations under the acts and regulations of Bermuda that are specific to MSB.

VII.2 Under Section 2 of the Anti-Terrorism (Financial and Other Measures) Act 2004 (ATFA), Section 2(1) of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 (POCA SEA) and Section 42A of the Proceeds of Crime Act 1997 (POCA), persons carrying on MSB within the meaning of Section 2(2) of the Money Service Business Act 2016 (MSB Act) are designated as AML/ATF Regulated Financial Institutions (RFI).

VII.3 Under Section 2(2) of the MSB Act, MSB means the business of providing any or all of the following MSB activities to the general public:

a) Money transmission services;
b) Cashing cheques that are made payable to customers and guaranteeing cheques;
c) Issuing, selling or redeeming drafts, money orders or traveller's cheques for cash;
d) Payment service business; and
e) Operating a bureau de change whereby cash in one currency is exchanged for cash in another currency.

VII.4 By amending the order, the Minister of Finance may add categories of MSB in addition to those set forth in paragraph VII.3.

VII.5 Nevertheless, where a company provides any of the services set forth in paragraph VII.3 as an ancillary service to its clients and does not levy a separate charge, the Bermuda Monetary Authority (Authority or BMA) is not likely to treat such an activity as being within scope of the MSB Act. Examples of such ancillary services include the cashing of hotel guests' personal cheques or the redemption of guests' traveller's cheques, or the cashing of customer cheques by a retailer. If there is any uncertainty or concern about the scope of this exemption, prospective applicants should contact the BMA to determine whether they are required to submit an application.

VII.6 Under Section 8 of the MSB Act, persons conducting MSB must obtain a licence from the BMA. Nevertheless, section 4(4) of the MSB Act sets forth that an institution carrying on MSB is not subject to the MSB Act if the institution is licensed under the Banks and Deposit Companies Act 1999. Such an institution is nonetheless an RFI subject to Bermuda's AML/ATF requirements unless it is exempted from the licensing requirement as described in paragraph VII.5.

VII.7 Under Section 9 of POCA SEA, all non-licensed RFIs must be registered with a competent authority. Where a person provides one of the services listed in paragraph VII.3, and does not obtain a licence from or register with another competent authority, that person is nonetheless an RFI which must register with the BMA.

VII.8 All RFIs must comply with the acts and regulations and with the general AML/ATF GN issued by the BMA.

VII.9 Schedule 1, Section 2(2) of the MSB Act sets forth that in determining whether an RFI is conducting its business in a prudent manner, the BMA will take into account any failure to comply, among other things, with:

a) The MSB Act;
b) The POCA;
c) The ATFA;
d) The Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 (POCR);
e) Relevant codes of practice issued by the BMA; and
f) International sanctions in effect in Bermuda.

VII.10 For the purposes of these guidance notes, the terms 'AML/ATF RFI' and 'RFI' should be understood to include persons conducting the MSB described in paragraph VII.3. The term 'MSB' should be understood to include all of the activities described in paragraph VII.3.

VII.11 RFIs conducting MSB should read these SSGN in conjunction with the general GN. This annex supplements but does not replace the general GN.

VII.12 Portions of this annex summarise or cross-reference relevant information that is contained in detail in the general GN. The detailed information in the general GN remains the authoritative guidance.

VII.13 Portions of this annex include sector-specific information, such as risk indicators that are particular to MSB. This sector-specific information should be considered as supplementary to the general GN.

Status of the guidance

VII.14 Pursuant to Section 49M of POCA and 120 of ATFA, these guidance notes are issued by the BMA under Section 5(2) of POCA SEA, approved by the Minister of Legal Affairs and available for download on the BMA website at www.bma.bm.

VII.15 These guidance notes are directly relevant to all senior management, including the compliance officer and the reporting officer. The primary purpose of the notes

is to provide guidance to those who establish and update the RFI's risk management policies, procedures and controls for the prevention and detection of Money Laundering (ML)/Terrorist Financing (TF).

VII.16 In determining whether a person is in breach of a relevant provision of the acts or regulations, the Supreme Court (Court) or the BMA is required to consider whether a person has followed any relevant guidance approved by the Minister of Legal Affairs and issued by the BMA. Requirements of the Court and the BMA are detailed in the provisions of Section 49M of POCA, POCR Regulation 19(2), Section 120 and paragraph 1(6) of Part I, Schedule I of ATFA and Section 20(6) of POCA SEA.

VII.17 When a provision of the acts or regulations is directly described in the text of the guidance, the guidance notes use the term '**must**' to indicate that the provision is mandatory.

VII.18 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.

VII.19 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.

VII.20 RFIs should be aware that under Section 16(1) of the Financial Intelligence Agency Act 2007, the Financial Intelligence Agency (FIA) may, while 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.

VII.21 Detailed information is set forth in the general GN, beginning with the **Preface**.

Senior management responsibilities and internal controls

VII.22 The AML/ATF responsibilities for senior management of an RFI conducting MSB are governed primarily by POCA, POCA SEA, ATFA and POCR Regulations 16 through 19.

VII.23 The AML/ATF internal control requirements for RFIs conducting MSB are governed primarily by Part 3 of the POCR Regulations.

VII.24 POCR Regulation 19 provides that failure to comply with the requirements of specified regulations is a criminal offence and carries with it significant penalties. On summary conviction, the penalty is a fine of up to $50,000. Where conviction occurs on indictment, penalties include a fine of up to $750,000, imprisonment for a term of two years or both.

VII.25 Section 20 of POCA SEA empowers the BMA to impose a penalty on any person supervised by the BMA in an amount up to $10 million for failure to comply with specified regulations. POCA SEA also provides for a number of criminal offences, including carrying on business without being registered pursuant to Section 9 of POCA SEA.

VII.26 Senior management of MSB RFIs should foster and promote a culture of compliance as a core business value. Senior management should ensure that an RFI is committed to identifying, assessing and effectively mitigating ML/TF risks when establishing or maintaining business relationships. Senior management should also ensure that adequate internal communication processes relevant to the actual or potential ML/TF risks faced by the MSB are appropriately implemented. In addition, senior management should understand all regulatory and supervisory requirements of the environment in which the MSB operates, including the MSB Act and other relevant acts and regulations.

VII.27 Under the acts and regulations of Bermuda, senior management in all RFIs must:

a) Ensure compliance with the acts and regulations;
b) Approve the RFI's policies, procedures and controls relating to its AML/ATF obligations;
c) Identify, assess and effectively mitigate the ML/TF risks posed by its customers, business relationships, countries or geographic areas, services, delivery channels, products and transactions;
d) Ensure that AML/ATF risk assessments remain documented, relevant and appropriate given the RFI's current 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) Screen employees 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) Independently audit and periodically test the RFI's AML/ATF policies, procedures and controls for effectiveness;
k) Ensure the RFI is prepared for compliance enquiries 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.

VII.28 RFIs must establish and maintain detailed policies, procedures and controls that are adequate and appropriate to forestall and prevent operations related to ML/TF.

VII.29 RFIs should consider using proven technology-driven solutions to minimise the risk of error and find efficiencies in their AML/ATF processes.

VII.30 Under Section 10(2)(c) of the MSB Act, an RFI must include its AML/ATF policies and procedures with its application for an MSB licence. RFIs should also submit a business risk assessment, client risk assessment and business plan at the time of application.

VII.31 Under Schedule 1, Section 5 of the MSB Act, an MSB must ensure that its position within the structure of any group to which it belongs does not obstruct the conduct of effective consolidated supervision.

VII.32 Where a Bermuda RFI conducting MSB has agents, 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 and must ensure that all such entities apply AML/ATF measures at least equivalent to those set out in the acts and regulations.

VII.33 Attempts to launder money through MSBs may be carried out in any one or several of three ways:

a) Externally, by a customer seeking to place, layer or integrate illicit assets;
b) Internally, by a director, manager, employee or agent, either individually or in collusion with others inside or outside the RFI conducting MSB; and
c) Indirectly, by a third-party service provider or an RFI, independent professional or other intermediary facilitating transactions involving illicit assets on behalf of another person.

VII.34 The majority of this annex addresses attempted ML by customers. ML risks involving agents and third parties are addressed in paragraphs VII.162 through VII.171. Money risks involving internal senior management, directors, managers or employees are addressed primarily via fit and proper requirements for MSB in paragraphs VII.40 through VII.44. The risks that MSBs may pose as customers of other RFIs are addressed in paragraphs VII.234 through VII.239.

VII.35 Specific requirements for an RFI's detailed policies, procedures and controls are set forth in **Chapters 1 through 11** of the general GN.

VII.36 Detailed information is set forth in Chapter 1: Senior Management Responsibilities and Internal Controls.

Links between MSB practices and AML/ATF policies, procedures and controls

VII.37 Persons carrying on MSB may be subject to acts and regulations creating requirements that achieve some of Bermuda's AML/ATF objectives. These acts and regulations include, but are not limited to, the MSB Act.

VII.38 Persons carrying on MSB may also be subject to the requirements, principles, standards and procedures set forth in guidance documents. These guidance

documents for MSB include but are not limited to:

a) Statement of Principles – Money Service Business Act 2016 (BMA – December 2016);
b) Code of Practice – Money Service Business Act 2016 (BMA – December 2016); and
c) Guidance Notes – Money Service Business Act 2016 (BMA – December 2016).

VII.39 The requirements of the acts, regulations and additional guidance documents described in paragraphs VII.37 through VII.38 provide a suitable foundation for the AML/ATF policies, procedures and controls that Bermuda RFIs are required to adopt and implement. Nevertheless, an RFI should not presume that its existing processes are sufficient. Each RFI must ensure that it meets each of its AML/ATF obligations under the relevant Bermuda acts, regulations and guidance notes, whether as part of its existing business processes or through separate processes.

Ownership, management and employee checks

VII.40 Licensing of any MSB is subject to the MSB's directors and officers meeting the fit and proper requirements set forth in Schedule 1 of the MSB Act (Minimum Criteria for Licensing.) As a cash-intensive business, it is also important that the persons employed by or appointed as agents of MSBs are of sound character and integrity.

VII.41 To guard against potential ML involving owners, directors, managers and employees of MSBs, POCR Regulation 18(1)(c) requires RFIs conducting MSB to screen such persons against high standards. Additional guidance on screening is set forth in paragraphs 1.73 through 1.77 of the general GN.

VII.42 RFIs should ensure that screenings are conducted both for the RFI itself and for any intermediary or third-party service provider.

VII.43 Where any screening is conducted by a third party, the RFI should have procedures to satisfy itself as to the effectiveness of the screening procedures the third party uses to ensure the competence and probity of each person subject to screening.

VII.44 Working with agents, intermediaries and third-party service providers that are licensed and that apply AML/ATF measures at least equivalent to those in Bermuda is likely to reduce the measures a Bermuda RFI conducting MSB will need to undertake in order to meet its screening obligations.

Monitoring and managing compliance

VII.45 RFIs must appoint a qualified and competent 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 the regulations are in place; and
b) Coordinate and monitor the compliance programme to ensure continuous compliance with the regulations.

VII.46 RFIs must also appoint a qualified and competent 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 the reporting officer has 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.

VII.47 The role, standing and competence of the compliance officer and the reporting officer, and the manner in which the RFI's policies, procedures and controls are designed and implemented directly impact the effectiveness of an RFI's AML/ATF arrangements, and the degree to which the RFI complies with the acts and regulations of Bermuda. For additional information on the roles and responsibilities of the compliance officer and reporting officer, see paragraphs 1.38 through 1.55 of the general GN.

Risk-based approach

VII.48 As described in **Chapter 2: Risk-Based Approach**, RFIs, including MSBs, must adopt a risk-based approach to managing ML/TF risks. In developing a business risk assessment and identifying and assessing the ML/TF risk to which they are exposed, MSBs should consider a range of factors, which may include:

a) The nature, scale, diversity and complexity of their business;
b) Target markets;
c) The number of customers already identified as high risk;
d) The jurisdictions the MSB is exposed to, either through its own activities or the activities of customers, especially in jurisdictions with relatively higher levels of corruption or organised crime, and those jurisdictions listed as higher risk by CFATF and FATF; and
e) The internal audit function and regulatory findings.

VII.49 The National Anti-Money Laundering Committee (NAMLC) has publicly released a report on Bermuda's national assessment of ML/TF risks. RFIs should take into account the results available to them from this and subsequent national risk assessments.

VII.50 RFIs should document and be able to justify the basis on which they have assessed the level of risk associated with each combination of customer, business relationship, country or geographic area, service, delivery channel, product or transaction.

VII.51 When designing and evaluating a new product or service, an RFI conducting MSB must, prior to launch, assess the risk of the product or service being used for ML/TF.

VII.52 Each RFI must ensure that its risk assessment methodology and the results of its risk assessments are documented, regularly reviewed and amended to keep them up to date, approved by senior management and available to be shared promptly with competent authorities.

VII.53 RFIs conducting MSB must employ a risk-based approach in determining:

a) Appropriate levels of CDD measures, including whether to apply enhanced CDD;
b) Risk-mitigation measures commensurate with the risks posed by the RFI's customers, business 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.

VII.54 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 and proliferation financing.

VII.55 The higher the risk an RFI faces from any particular combination of customer, business relationship, country or geographic area, service, delivery channel, product or transaction, the stronger and/or more numerous the RFI's mitigation measures must be.

VII.56 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.

VII.57 An RFI's assessments of the ML/TF risks associated with a customer or transaction should be conducted independently and in a manner that demonstrates high standards of professionalism extending beyond simply fulfilling the requirements of the acts and regulations.

VII.58 RFIs should consider whether the Financial Action Task Force (FATF) or Caribbean Financial Action Task Force (CFATF) has made available information indicating that a country or territory is high risk. RFIs should also conduct their

own due diligence to determine what other countries or territories represent a high risk for ML, TF, corruption or international sanctions.

VII.59 Although RFIs conducting MSB should target compliance resources toward higher-risk situations, they must also continue to apply risk mitigation measures to any 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.

VII.60 Detailed information on the requirement that RFIs use a risk-based approach to mitigate the risks of being used in connection with ML/TF is set forth in **Chapter 2: Risk-Based Approach**.

VII.61 Using the risk-based approach, each RFI conducting MSB should determine its risk tolerance, which is the amount of ML/TF risk the RFI will accept in pursuit of its business goals.

VII.62 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 effectively manage the risks it decides to accept.

VII.63 Nothing in the acts or regulations prevents an RFI from deliberately choosing to accept higher-risk business. Each RFI must, however, ensure that it has the capacity and expertise to apply risk mitigation measures that are commensurate with the risks it faces and that it does effectively apply those measures.

VII.64 The MSB sector is often considered as posing a high risk of ML/TF. Criminals may be attracted to the sector because:

a) Money service transactions are often fast, simple and characterised by certainty and finality;
b) Money services often involve cash and bearer instruments;
c) Money services may be cross-border, with a global reach;
d) Money service transactions are often one-off transactions, taking place outside of an established business relationship that could be more readily monitored for uncharacteristic behaviour;
e) MSB transactions may be characterised by a low frequency of contact between customers and the MSB;
f) Some money services could be used to facilitate anonymity or to exploit a false identity; and
g) Where MSB involves agents, there is a risk that an agent will not properly follow appropriate AML/ATF policies, procedures and controls.

VII.65 Although some MSBs may be abused by criminals for ML/TF purposes, not all MSBs are inherently high-risk for ML/TF.

VII.66 The level of inherent risk associated with MSB depends upon a number of factors, including, but not limited to the:

a) Size of the MSB;
b) Products and services the business offers;
c) Extent to which branches and agents are involved in the business;
d) Complexity of any payment chains used;
e) Geographic areas in which the business operates; and
f) Identity and geographic origin of the business' customers.

VII.67 The level of inherent ML/TF risk may be lower where the MSB:

a) Primarily markets to customers conducting routine transactions with moderate frequency in low amounts;
b) Is an established business with a known operating history;
c) Is a money transmitter that only remits funds to domestic entities;
d) Offers only a single MSB product or service; or
e) Processes both sides of a transaction primarily for local residents.

VII.68 Where a MSB offers only a single product or service, the business's risk assessment must nonetheless identify categories of customers, transactions and conduct that are higher or lower risk within that single product or service.

VII.69 The level of inherent ML/TF risk may be higher where the MSB:

a) Deals significantly in cross-border transactions or one-off transactions that are frequent and/or large in amount;
b) Offers several money services; or
c) Is located in, transacts with or through, or otherwise has a connection with a geographic area considered to be high risk for ML/TF or other criminal activity (see paragraphs 5.17 through 5.19 of the general GN).

VII.70 ML/TF risks associated with MSB can be reduced through the application of mitigation measures that are tailored to the risks the business identifies.

VII.71 Examples of measures that may be used to mitigate ML/TF risk that an RFI has identified include, but are not limited to:

a) Attainment and verification of additional customer information;
b) Usage limits for the RFI's products and services;
c) Geographic limits on the use of the RFI's products and services;
d) Segmentation of due diligence and controls; and
e) Increased monitoring and record-keeping.

VII.72 The mitigation measures noted in paragraph VII.71 are detailed in the context of new payment methods in paragraphs 5.36 through 5.95 of the general GN.

VII.73 When identifying ML/TF risk factors, questions that MSB RFIs should consider when evaluating customer risks include whether:

a) Customers are companies, partnerships or trusts;
b) The RFI undertakes business in areas with a highly transient population;
c) The customer base is stable or has a high turnover;
d) The RFI is acting for international customers or customers with whom the RFI's employees do not have face-to-face contact;
e) The RFI accepts business from abroad, particularly from customers based in, or whose beneficial owners are based in, tax havens, countries with high levels of corruption or countries where terrorist organisations operate (see paragraphs 5.17 through 5.19 of the general GN);
f) The RFI acts for entities that have a complex ownership structure or cross-border operations;
g) The RFI accepts payments that are made to or received from third parties;
h) The RFI accepts occasional transactions outside of an established business relationship;
i) A customer's patterns of transactions or conduct, or changes to a customer's patterns of transactions or conduct, pose an ML/TF risk; and
j) The RFI is taking appropriate steps to confirm that customers introduced by an agent or third party have been identified and verified as required by Bermudian acts and regulations.

VII.74 Specific indicators of higher risk in MSB are discussed in detail in paragraphs VII.242 through VII.247.

Customer due diligence

VII.75 RFIs conducting MSB must carry out Customer Due Diligence (CDD).

VII.76 Detailed information on CDD is set forth in **Chapters 3, 4 and 5** of the general GN and paragraphs VII.75 through VII.180 of this annex.

VII.77 Carrying out CDD allows RFIs to:

a) Guard against impersonation and other types of fraud by being satisfied that customers are who they say they are;
b) Know whether a customer or person associated with a customer is acting on behalf of any unknown or unexpected person;
c) Identify any legal barriers (e.g., international sanctions) to providing the product or service requested;
d) Maintain a sound basis for identifying, limiting and controlling risk exposure;
e) Avoid committing offences under POCA and ATFA relating to ML/TF; and
f) Assist law enforcement agencies and authorities by providing information on

MSB customers or activities being investigated.

VII.78 CDD measures that must be carried out include:

a) Identifying and, in most cases, verifying the identity of each customer;
b) Understanding the nature of the customer's business and the purpose and intended nature of the customer's business relationship with the RFI;
c) Identifying the source of wealth and source of funds associated with the customer;
d) Collecting information about the legal powers that regulate and bind a customer that is a legal person or legal arrangement;
e) Identifying and verifying signatories, directors and other persons exercising control over the management of the customer or its relationship with the RFI;
f) Identifying and taking adequate measures on a risk-sensitive basis to verify the identity of the beneficial owner(s) or the customer;
g) 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; and
h) Updating the CDD information at appropriate times. This includes ensuring that information on the ultimate beneficial owners and/or controllers of companies, partnerships and other legal entities is known to the RFI, properly updated and recorded.

VII.79 The extent of CDD measures must be determined using a risk-based approach. 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.

VII.80 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.

VII.81 Detailed information on CDD for natural persons is set forth in paragraphs 4.5 through 4.60 of the general GN.

VII.82 Detailed information on CDD for legal persons and other legal arrangements is set forth in paragraphs 4.61 through 4.153 of the general GN and Annex I.

<u>Nature of the customer's business and purpose and intended nature of the business relationship</u>

VII.83 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 such that the business relationship can be effectively monitored.

VII.84 In many instances, an MSB customer will be a natural person. An MSB customer that is a legal person or other legal arrangement may pose a higher inherent risk for ML/TF. For customers that are not natural persons, and particularly for customers that provide money services or are agents for money services, an RFI should collect information, including, but not limited to:

a) The customer's goals for the MSB relationship or transaction;
b) The source of wealth and source of funds to be used in the MSB relationship or transaction;
c) The anticipated type, volume, value, frequency, duration and nature of the activity that is likely to be undertaken through the MSB relationship or transaction;
d) The geographic connections of the customer and each beneficial owner, administrator, advisor, operator, employee, manager, director or other person who is able to exercise significant power over the MSB relationship or occasional transaction;
e) The means of payment (cash, wire transfer, other means of payment);
f) Whether there is any bearer arrangement, mail holding arrangement or care of (c/o) mail arrangement and, if so, the reasons for and details of the arrangement; and
g) Whether any payments are to be made to or by third parties and, if so, the reasons for and details of the request.

<u>One-off transactions, occasional transactions and business relationships</u>

VII.85 To properly apply CDD, RFIs should distinguish between one-off transactions, occasional transactions and transactions that take place as part of an ongoing business relationship.

VII.86 The term 'one-off transaction' means a transaction carried out outside of a business relationship, regardless of the amount of the transaction.

VII.87 The term 'occasional transaction' means a one-off transaction 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 or money transmission carried out in an amount greater than $1,000. The values described in this paragraph refer to the gross value of the transaction, not including the value of any commissions, fees or charges.

VII.88 The regulations define a 'business relationship' as a business, professional or commercial relationship between an RFI and a customer, which, at the time contact is first made, the RFI expects to have an element of duration. A business relationship is also formed where the expectation of duration is not initially present but develops over time. A business relationship need not involve the RFI in an actual transaction; giving advice may often constitute the establishment of a business relationship.

VII.89 Many MSBs carry out one-off transactions for customers that are outside of an ongoing business relationship. Nevertheless, an RFI's introduction of a customer loyalty programme, relationship management tool or linkages with other financial services, when coupled with an agreement between the RFI and the customer, indicates that a business relationship has been formed.

VII.90 Where a business relationship has been formed, an RFI must apply full CDD measures to the relationship.

VII.91 Where a one-off transaction is $1,000 or less and is assessed as being low risk for ML/TF, information based on a brief conversation with, or knowledge of, a natural person customer may be sufficient. See paragraphs VII.119 through VII.133 and paragraph VII.179.

VII.92 Where a one-off transaction or business relationship involves more than $1,000 or is of a commercial nature, and particularly where the customer is a legal person or legal arrangement, formal CDD measures must be applied and recorded in accordance with the regulations and these guidance notes.

Linked transactions

VII.93 Linked transactions may be a series of transactions involving a customer, and/or they may be transactions that appear to be independent but are split into two or more transactions to avoid detection, CDD requirements or questions about the source of wealth and/or source of funds.

VII.94 RFIs should have systems to identify and detect linked transactions, apply enhanced due diligence to them, and report any suspicious activity. These systems should identify a series of transactions from one customer to one or more recipients over a period of time, and they should identify a series of transactions from several customers to the same recipient over a period of time.

VII.95 An RFI's systems must be able to identify linked transactions that are conducted through any and all of the RFI's branches and agents.

VII.96 Transactions separated by a rolling interval of three months or more need not be treated as linked, provided there is no other evidence of a link and the transactions do not otherwise give rise to a business relationship.

Source of wealth and source of funds

VII.97 Enquiries regarding the source of wealth and source of funds are among the most useful sources of information leading to knowledge, suspicion or reasonable grounds for suspicion that funds or assets are criminal property or that a person is involved in ML/TF.

VII.98 RFIs should make enquiries as to how a customer has acquired the wealth, whether in currency, securities or any other assets, to be used with regard to the MSB relationship or transaction.

VII.99 The extent of such enquiries to understand and determine the legitimacy of a customer's source of wealth and source of funds should be made using a risk-based approach. Where a proposed one-off transaction is small and is assessed as low-risk for ML/TF, or where the source of wealth or funds is readily apparent, such enquiries may be limited in accordance with the RFI's AML/ATF policies, procedures and controls. Where a potential or existing customer, business relationship or transaction is assessed as higher risk, the RFI must undertake more thorough and more frequent measures to understand and confirm the source of wealth and source of funds.

VII.100 RFIs should also ensure that they understand the specific means of payment, including the details of any account that a customer proposes to use.

VII.101 Additional information on the source of funds and source of wealth is set forth in paragraphs 5.110 through 5.113 of the general GN.

Definition of 'customer' in an MSB context

VII.102 An RFI's customer is generally a private natural person, legal person, trust or other legal arrangement with or for whom a business relationship is established, or with or for whom an occasional transaction is carried out. A given MSB relationship or transaction may have more than one person who is a customer.

VII.103 A customer that is not a private natural person generally involves a number of natural persons, such as the directors, trustees, beneficial owners and other persons who directly or indirectly own or have the ability to control the customer. An RFI's customer is not only the customer entity or arrangement itself but also the natural persons who comprise the entity or arrangement and its relationship with the RFI.

VII.104 Where a one-off transaction or business relationship involves multiple parties, such as when money is being transmitted with the involvement of one or more agents, any agent may also be a customer.

VII.105 For the purposes of these guidance notes, a customer includes each of the following:

a) Each private natural person, legal person, trust or other legal arrangement that is or comprises a customer seeking an MSB product or service;
b) Each agent involved in a business relationship or one-off transaction; and
c) Each beneficial owner of a customer.

VII.106 Where an RFI has reason to believe that a customer is acting on behalf of another

person, that other person is also a customer.

VII.107 Where a customer is an agent acting on behalf of a principal other than the RFI conducting CDD, the principal must also be subject to CDD, including identifying and verifying the principal as a customer, and identifying and taking reasonable measures to verify the persons who own and control the principal and its management.

VII.108 Full information on the meaning of customer, business relationship and occasional transaction, and on identifying and verifying natural persons, legal persons, trusts and other legal arrangements is set forth in **Chapter 4: Standard CDD Measures**.

Definition of beneficial owner in an MSB context

VII.109 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 own and control a customer.

VII.110 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.

VII.111 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 4.48 of the general GN.

VII.112 Where a customer is a legal person or legal arrangement, 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 who are entitled to a specified interest in the property of the trust or other legal arrangement.

VII.113 Where control or ownership of a customer is held by another legal person or legal arrangement, RFIs should consider as a beneficial owner each private natural person who ultimately controls or owns that other legal person or legal arrangement.

VII.114 RFIs must consider as beneficial owners those persons who own or control a customer or its management, directly or indirectly, through any bearer or nominee arrangement.

VII.115 Information on the identification and verification of beneficial owners is set forth in POCR Regulation 3 and **Chapter 4: Standard CDD Measures**.

Obtaining and verifying customer identification information

VII.116 RFIs must obtain and verify identification information for each person who is a customer in the MSB context.

VII.117 A person who is a customer in the MSB context may be a natural person, a legal person, a trust or other legal arrangement. For each type of customer, RFIs should follow the identification and verification requirements in **Chapter 4: Standard CDD Measures**, as supplemented by any relevant annexes.

VII.118 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 in accordance with **Chapter 11: Record-Keeping**.

Standard identification requirements for natural persons

VII.119 Where a customer forms a business relationship with an RFI, the RFI must obtain and verify identification information for that person, applying, at a minimum, standard identification requirements.

VII.120 Where the customer has not formed a business relationship with the RFI and is instead engaging in a one-off transaction, the customer identification requirements may differ on the basis of the type of transaction, the size of the transaction and whether the transaction is linked with other transactions.

VII.121 Where a one-off transaction is an occasional transaction as defined in paragraph VII.87, an RFI must apply, at a minimum, the standard CDD measures.

VII.122 An RFI fulfils the standard identification requirements by obtaining a natural person's:

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;
f) Gender; and
g) Personal identification number or other unique identifier contained in a valid government-issued document.

VII.123 In addition, to fulfil the standard identification requirements for natural persons, an RFI must verify the following information using appropriate documentary or electronic means:

a) Full legal name;
b) Principal residential address; and
c) Date of birth.

Simplified identification requirements for natural persons

VII.124 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 considering the results of Bermuda's national risk assessment and the risk assessments carried out by the RFI. Any application of simplified identification requirements is permissible only where:

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.

VII.125 Where an RFI carries out any wire transfer or other money transmission in an amount exceeding $1,000, the RFI must apply the standard CDD measures, as such a transaction is an occasional transaction.

VII.126 The following MSB activities frequently do not involve a wire transfer or other money transmission that would require standard CDD measures for one-off transactions in amounts greater than $1,000 but less than $15,000:

a) Cashing and guaranteeing cheques;
b) Issuing, selling or redeeming drafts, money orders or traveller's cheques for cash; and
c) Operating a bureau de change.

VII.127 RFIs should nonetheless determine whether any of the MSB activities listed in paragraph VII.126, whether alone or in combination with another product or service the RFI offers, does in fact involve a wire transfer or money transmission that would require the application of standard CDD measures.

VII.128 Where an RFI carries out a one-off transaction that is a wire transfer or money transmission of $1,000 or less, simplified due diligence may be permissible, depending on the RFI's reasonable and documented risk assessment.

VII.129 Where an RFI conducting MSB has confirmed that a particular one-off transaction in an amount less than $15,000 does not involve a wire transfer or money transmission and that the transaction and customer are low risk for ML/TF, the RFI is not automatically required to conduct CDD for the customer.

VII.130 Where simplified due diligence is permissible, RFIs should nonetheless obtain and verify the identity of customers for all MSB transactions unless the RFI has documented a probability that the application of standard CDD requirements will drive a class of legitimate customers to transact outside of the regulated financial

sector, or will cause a class of legitimate customers to be unable to access the service in question by any means.

VII.131 Where a transaction involves an entity for which simplified due diligence is appropriate, RFIs must adhere to the regulations and guidance notes in identifying and verifying signatories and other persons connected with the customer.

VII.132 Bearing in mind the above, an RFI's AML/ATF risk assessment may inform the RFI's establishment of transactional thresholds, customer profiles or other criteria to establish customer identification procedures under the RFI's AML/ATF policies, procedures and controls.

VII.133 Paragraphs VII.119 through VII.132 set forth that in the context of MSB, a one-off transaction in an amount less than $15,000 that does not involve a wire transfer or money transmission may be eligible for simplified CDD. Nevertheless, an RFI's risk assessment may cause the RFI to conduct CDD where risks that are present are not effectively mitigated through other means. For example, as discussed in paragraphs VII.148 through VII.151, an RFI may determine that it is necessary to conduct CDD on occasional transactions that involve cash, bearer instruments or other higher-risk criteria.

Enhanced due diligence for MSB

VII.134 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.

VII.135 Under POCR Regulation 11, 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 country or geographic location of counterparties with which the customer engages are assessed as higher than standard.

VII.136 In the context of MSB, the involvement of agents in the provision of an RFI's services may require an RFI to apply enhanced due diligence to its own agent network.

VII.137 In addition, the use of new payment methods in the context of MSB may require an RFI to apply enhanced due diligence. Risk factors common to many new payment methods 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 a new payment method's system; and
h) The use of service providers or agents that are not subject to effective AML/ATF regulation.

VII.138 Additional information on enhanced due diligence for new payment methods is set forth in paragraphs 5.36 through 5.93 of the general GN.

VII.139 Enhanced due diligence must be applied in each of the following circumstances:

a) The customer has not been physically present for identification purposes (see paragraph 5.25 through 5.29 of the general GN);
b) The business involves a correspondent banking relationship (see paragraph 5.148 of the general GN);
c) The business relationship or occasional transaction involves a Politically Exposed Person (PEP) (see paragraphs 5.96 through 5.116 of the general GN);
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; or
e) There is any other situation that, by its nature, may present a higher risk of ML/TF.

VII.140 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 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, a 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.

VII.141 For the purposes of paragraph 5.18 of the general GN, a person associated with the business relationship or occasional transaction is any of the following:

a) A customer;
b) A beneficial owner or controller of the customer;
c) A third party for whom the customer is acting;

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

VII.142 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.

VII.143 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 of the general GN);
c) Additional information on the customer's source of funds and source of wealth (see paragraphs 5.110 through 5.113 of the general GN);
d) Additional information on the reasons for planned or completed transactions; and
e) Approval of senior management to carry out a one-off transaction or to commence or continue the business relationship (see paragraph 5.109 of the general GN).

VII.144 In addition, RFIs should consider applying additional measures, such as:

a) More frequently updating the identification and verification data for the customer or agent, any beneficial owner(s) and any other persons with an ownership or controlling interest in the customer or agent, or persons who otherwise exercise significant influence or control over the customer or agent or its business relationship with the RFI;
b) Conducting enhanced ongoing monitoring of the agent or customer business relationship by increasing the number and frequency of controls applied and identifying patterns of transactions or other activity requiring further examination.

VII.145 Additional mitigation measures are set forth in paragraphs VII.71 and 5.36 through 5.93 of the general GN.

VII.146 Detailed information on enhanced due diligence is set forth in **Chapter 5: Non-Standard CDD Measures**.

VII.147 Specific indicators of higher risk in MSB are discussed in greater detail in paragraphs VII.241 through VII.246 of this annex.

<u>Customer transactions involving cash or bearer instruments</u>

VII.148 Many RFIs conducting MSB handle cash or bearer instruments, which may easily be abused for criminal purposes. Due to the higher inherent risk of ML/TF where cash or bearer instruments are involved, RFIs must ensure that the inherent risks are identified, evaluated and mitigated using appropriate AML/ATF measures.

VII.149 While some transactions below $15,000 may not automatically require the application of standard CDD, an RFI's AML/ATF risk assessment may determine the use of cash or bearer instruments in such transactions or the involvement of other higher risk factors requires the RFI to conduct CDD.

VII.150 Paragraph 7.14 states that each RFI should establish norms for cash transactions and procedures for the identification of unusual cash transactions or proposed cash transactions.

VII.151 Paragraphs 4.99 through 4.103 provide additional guidance on the use of bearer instruments.

Timing of customer due diligence

VII.152 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 or money transmission in an amount of $1,000 or more (see Chapter 8: Wire Transfers);
c) Suspects ML/TF;
d) Doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification; or
e) Has committed to doing so under the RFI's risk-based AML/ATF policies, procedures and controls (e.g., when the RFI has committed to applying CDD for one-off transactions in an amount below $15,000 that are not wire transfers or money transmissions).

VII.153 Where the product or service is a one-off transaction amounting to less than $15,000, the RFI should apply CDD measures at the time the one-off transaction is entered into.

VII.154 Nevertheless, where a customer who has carried out a one-off transaction amounting to less than $15,000 requests a future or ongoing service, the RFI should have policies it uses to consider whether the transactions are linked and whether it is entering into a business relationship requiring CDD measures.

VII.155 Without exception, RFIs conducting MSB should always identify the customer before the establishment of a business relationship or the carrying out of an occasional transaction.

VII.156 Verification should take place:

a) Before the RFI establishes a new business relationship or, in limited circumstances where essential to avoid interrupting normal conduct of business during the establishment of a new business relationship;
b) Before the RFI provides any service as part of a business relationship or occasional transaction; and
c) Subsequently, when there is any change in information previously provided or when otherwise deemed necessary due to information obtained through risk assessment or ongoing monitoring.

VII.157 Detailed information on the timing of CDD measures is set forth in **Chapter 3: Overview of Customer Due Diligence**.

Refusing or terminating MSB

VII.158 If for any reason an RFI is unable to complete CDD measures in relation to a customer, POCR Regulation 9 establishes that the RFI must:

a) In the case of a proposed business relationship or transaction, not establish that business relationship, not open any account and not carry out any transaction with or on behalf of the customer;
b) In the case of an existing business relationship, terminate that business relationship with the customer; and
c) Consider whether the RFI is required to make a suspicious activity report to the FIA in accordance with its obligations under POCA and ATFA.

VII.159 Where an RFI conducting MSB decides that a business relationship must be terminated due to an inability to complete CDD, the RFI must take appropriate steps to end the business relationship or, as appropriate, not proceed with any proposed act, account, service, transaction or representation. Where there are no grounds for filing a suspicious activity report, any customer funds should be returned to the customer by bank transfer, wherever possible, into the customer's bank account from which the RFI originally received the funds.

VII.160 Regardless of whether an RFI is an originating, intermediary or beneficiary RFI of any wire transfer or money transmission, it must have effective risk-based policies and procedures for determining when to execute, reject or suspend the wire transfer or money transmission and the capacity to timely effectuate any rejection or suspension.

VII.161 Where an RFI declines or terminates business due to knowledge, suspicion or reasonable grounds for suspicion that the business might be criminal in intent or origin, the RFI must refrain from referring such declined business to another person.

Agent networks and other third parties

VII.162 Where an RFI's MSB involves an agent network or other third parties, RFIs should ensure that the agent or other third party has in placeappropriate policies, procedures and controls to assess and mitigate the ML/TF risks associated with their involvement in the MSB.

VII.163 RFIs should require agents and other third parties to demonstrate that they are effectively supervised for compliance with appropriate AML/ATF obligations.

VII.164 An RFI may have a range of contractual relationships with agents or third parties. Some agents may be considered employees or otherwise as an integral part of the RFI and, therefore, directly subject to the RFI's AML/ATF policies, procedures and controls. Other agents may be considered wholly separate entities upon which the RFI seeks to rely for purposes of AML/ATF. Still, other agents may be most accurately considered as customers entering into a business relationship with the RFI, for which appropriate CDD must be conducted. Each RFI must ensure that this range of possible relationships does not prevent the effective implementation of appropriate AML/ATF controls at all levels of any agency structure or multi-party payment chain.

VII.165 RFIs that provide services with the involvement of other parties must determine the distribution of AML/ATF responsibilities between the parties.

VII.166 Regardless of the type of relationship the RFI has entered into with the agent or other third party, the RFI should ensure that the following steps are taken with regard to each agent:

Prior to on-boarding the agent:

a) Require the agent to demonstrate that it is properly licensed, registered and supervised for compliance with appropriate AML/ATF obligations;
b) Require the agent to provide the information set forth in paragraph VII.171, which the RFI must include in its agent list;
c) Conduct a beneficial ownership assessment, including fit-and-proper testing and a review of negative media;
d) Conduct a criminal background check of the agent's ownership, management and relevant employees;
e) Verify any required compliance credentials of relevant employees; and
f) Review the agent's AML/ATF policies, procedures and controls, and ensure that the distribution of AML/ATF responsibilities is in line with the requirements of these guidance notes.

After on-boarding, the agent must:

a) Train the agent on the RFI's AML/ATF policies, procedures and controls;
b) Conduct ongoing monitoring of transactions and business relationships

involving the agent;
c) Conduct ongoing monitoring and testing of the agent's compliance with the relevant AML/ATF policies, procedures and controls;
d) Consider whether on-site visits and/or testing are merited;
e) Take prompt corrective action as needed, including filing suspicious activity reports about the agent where appropriate; and
f) Terminate the relationship where appropriate.

VII.167 Where an RFI outsources tasks to an agent, the agent is an extension of the RFI. Similarly, where the RFI providing the product or service has a direct sales force, that sales force is considered to be part of the RFI, regardless of whether it operates under a separate group legal entity. In such cases, the RFI retains full responsibility for implementing group-wide AML/ATF policies, procedures and controls. While the RFI's agent may obtain and verify CDD evidence, it is the responsibility of the RFI itself to advise and train the agent and to conduct ongoing monitoring of the agent and its transactions.

VII.168 Where, however, a third party is not an agent but is instead a person or institution with its own AML/ATF policies, procedures and controls upon which the RFI wishes to rely for AML/ATF purposes, such reliance is permissible only in specified circumstances.

VII.169 Paragraphs 5.117 through 5.148 of the general GN set forth the circumstances in which reliance on a third party is permissible. Paragraphs 3.23 through 3.25 of the general GN provide additional relevant guidance. In any reliance situation, however, the relying RFI retains responsibility for any failure to comply with a requirement of the regulations, as this responsibility cannot be delegated.

VII.170 RFIs conducting MSB should ensure that each natural or legal person working for the RFI as an agent is licensed or registered by a competent authority that operates and effectively supervises compliance with an appropriate AML/ATF regulatory regime.

VII.171 Where an RFI's agent is not licensed or registered or cannot be licensed or registered with a competent authority, the RFI should maintain a current list of its agents and make that list available to the BMA upon request. Such an agent list should include, at a minimum:

a) The agent's name, including any trade name(s);
b) The agent's business and (if different) mailing address;
c) The agent's telephone number;
d) The types of services the agent provides on behalf of the RFI;
e) The agent's monthly gross transaction amount for the previous 12 months;
f) The year the RFI accepted the agent as such;
g) The name and address of any bank at which the agent maintains an account used in the agent's MSB on behalf of the RFI; and
h) The number, if any, of branches or sub-agents the agent has.

Money transmission and wire transfers

VII.172 In the context of MSB, any money transmission is a wire transfer and subject to the rules for wire transfers set forth in POCR Regulations 21 through 31A and **Chapter 8: Wire Transfers**. An objective of the regulations and guidance is to increase the transparency of all transfers of funds, both cross-border and domestic, by requiring RFIs to include essential information with each transfer.

VII.173 RFIs conducting wire transfers or money transmissions must ensure that complete information on both the payer and payee accompanies each cross-border transfer of funds over $1,000 and each cross-border transaction that is carried out in several operations that appear to be linked and together exceed $1,000.

VII.174 Complete information on the payer means:

a) The payer's name;
b) The payer's address; and
c) The payer's account number.

VII.175 Complete information on the payee means:

a) The payee's name; and
b) The payee's account number.

VII.176 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.

VII.177 Where a payer or payee does not have an account number, the payment service provider must substitute it with a unique identifier that allows the transaction to be traced to the payee. See paragraph 8.33 of the general GN.

VII.178 MSB RFIs should allow substitutions described in paragraphs 8.11 and 8.12 of the general GN 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 MSB RFI 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 of the general GN to other RFIs involved in the execution of the transfer.

VII.179 Where the payer does not have a business relationship with the RFI and the wire transfer or money transmission is $1,000 or less, the payer RFI should obtain information establishing the payer's identity and address. Where the address is substituted with a payer's date and place of birth or with a payer's national identity number, that customer information should be obtained. RFIs are not

required to verify the information obtained for such transactions; nonetheless, it is advisable to do so in all cases unless the RFI has documented a probability that the application of standard CDD requirements will drive a class of legitimate customers to transact outside of the regulated financial sector or will cause a class of legitimate customers to be unable to access the service in question by any means. Where a transaction is carried out in several operations that appear to be linked and together exceed $1,000, the verification requirements described in paragraphs VII.123 and VI.156 apply.

VII.180 Additional detail concerning wire transfers and money transmission is set forth in **Chapter 8: Wire Transfers**.

International sanctions

VII.181 RFIs conducting MSB should implement a sanctions compliance programme in line with the guidance set forth in **Chapter 6: International Sanctions**.

VII.182 RFIs should have processes in place for screening against sanctions list agents, customers, prospective customers and any third-party intermediaries seeking to introduce new business, and processes for performing background checks to identify information about an agent's or customer's association with financial or other crime and with PEPs.

VII.183 RFIs should determine whether any persons connected with an agent or customer and the natural persons connected with any such persons that are legal entities, trusts or other legal arrangements are sanctions targets.

VII.184 RFIs must be aware that, in contrast to AML/ATF measures, which permit MSBs some flexibility in setting their own timetables for verifying (see POCR Regulation 8) and updating CDD information (see POCR Regulations 6(2) and 7(2)(c)), an RFI risks breaching a sanctions obligation as soon as a person, entity, good, service or activity 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.

Ongoing monitoring

VII.185 POCR Regulations 6(3), 6(3A), 7, 11(4)(c), 12(1)(b), 13(4), 14(A)(2)(d), 16 and 18 require RFIs to conduct ongoing monitoring of the business relationship with their customers.

VII.186 RFIs conducting MSB should also conduct ongoing monitoring and testing of each agent's compliance with relevant AML/ATF policies, procedures and controls.

VII.187 Ongoing monitoring in the context of MSB supports several objectives:

a) Maintaining a proper understanding of an agent or customer's owners, controllers and activities;
b) Ensuring that CDD documents and other records are accurate and up to date;
c) Providing accurate inputs for the RFI's ongoing risk assessment processes;
d) Testing the outcomes of the RFI's ongoing risk assessment processes; and
e) Detecting and scrutinising unusual or suspicious conduct in relation to an agent or customer.

VII.188 Ongoing monitoring of an agent or customer business relationship includes:

a) Employing the RFI's professional experience and judgement in the formulation of suspicions, where appropriate;
b) 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 agent's or customer's conduct are consistent with the RFI's knowledge of the agent or customer, the agent or customer profile, and the persons who own, control and act on behalf of the agent or customer;
c) Investigating the background and purpose of all complex or unusually large transactions, patterns of transactions that have no apparent economic or lawful purpose, and unusual corporate or other legal structures;
d) When handling customer funds or accounts in a fiduciary capacity, monitoring the frequency and size of customer transactions or funds transfers to detect turnover that is out of line with the customer's declared profile;
e) Recording in writing the findings of investigations;
f) Determining whether an agent, customer or person connected with an agent or customer is a PEP and whether an agent or customer relationship involves a country 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;
g) Reviewing existing documents, data and information to ensure that they are accurate, up to date, adequate and relevant for the purpose of applying CDD measures in the context of MSB; and
h) Adjusting risk profiles and risk assessments based on the information reviewed.

VII.189 Ongoing monitoring must be carried out on a risk-sensitive basis. The inherent ML/TF risk levels associated with MSBs should be considered when determining baseline levels of ongoing monitoring. Higher-risk customers, transactions and business relationships must be subjected to enhanced due diligence and more frequent and/or intensive ongoing monitoring.

VII.190 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 in relation to MSB agents and customers and the persons who own and control those

customers. See paragraphs 7.11 through 7.14 of the general GN.

VII.191 Once an RFI has established norms for lawful transactions and conduct, it must monitor the business relationship, including transactions, patterns of transactions and conduct by customers and the persons who own, control and act on behalf of those customers to identify transactions and conduct falling outside of the norm.

VII.192 The determination of norms for a category of customers or a category of persons who own, control or act on behalf of a customer should be based initially upon the information obtained to understand the nature of the customer's business and the purpose and intended nature of the business relationship with the RFI. See paragraphs VII.83 through VII.84.

VII.193 In determining a proper allocation of monitoring resources, RFIs should consider:

a) The size and complexity of the RFI;
b) The nature, scope and delivery channels of the products and services the RFI provides;
c) Any national risk assessment findings;
d) The RFI's own risk assessment findings; and
e) The nature, scope and effectiveness of the RFI's existing monitoring systems.

VII.194 With respect to an agent or customer, RFIs should consider:

a) The nature, amount and frequency of the transactions;
b) Geographic connections (see paragraph 2.50 of the general GN);
c) Whether the agent or customer is known to offer or use other products and services;
d) Whether the agent or customer can be categorised according to activity or turnover and whether the agent or customer's conduct falls outside any norms established for any categories identified; and
e) Whether the agent or customer presents a higher than standard risk for ML/TF.

VII.195 Failure to adequately monitor an agent or 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.

VII.196 Monitoring may take place both in real time and after the event, and it may be both manual and automated. Irrespective, any system of monitoring should ensure at its core that:

a) Customers, persons who own, control and act on behalf of customers, 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.

VII.197 The adequacy of an MSB's monitoring system, and the criteria used to determine the level of monitoring to be implemented, should be reviewed regularly to ensure that they are in line with the MSB's AML/ATF policies, procedures and risk assessments. Transaction monitoring systems may be manual or automated depending on the volume of transactions an MSB processes; however, where automated systems are used, MSBs should understand each system's operating rules, verify each system's integrity on a regular basis and confirm that the systems collectively provide appropriate monitoring for all identified ML/TF risks.

VII.198 An RFI should calibrate its monitoring systems to identify for review all higher-risk activity, including, but not limited to:

a) Transactions or conduct falling outside of the expected norm for a customer, product or service;
b) All complex or unusually large transactions and unusual patterns of transactions that have no apparent economic or lawful purpose;
c) Transactions for which the customer has not been physically present for identification purposes (see paragraphs 5.25 through 5.29 of the general GN);
d) Business involving a correspondent banking relationship (see paragraph 5.148 of the general GN);
e) A business relationship or occasional transaction involving a PEP (see paragraphs 5.96 through 5.116 of the general GN);
f) A business relationship or occasional transaction that has a connection with a country or territory that represents a higher risk of ML, corruption, TF or being subject to international sanctions (see paragraphs 5.17 through 5.19 of the general GN);
g) Transactions that may favour anonymity, including new payment methods (see paragraphs 5.36 through 5.93 of the general GN); and
h) Transactions with regard to an agent of the RFI not having followed the requisite AML/ATF policies, procedures and controls.

VII.199 Where an RFI accepts higher-risk business, it must ensure that it has the capacity and expertise to effectively conduct ongoing monitoring of the customer or agent, the persons who own, control and act on behalf of the customer or agent and the business relationship with the RFI. See paragraph VII.63.

VII.200 Detailed information on ongoing monitoring is set forth in **Chapter 7: Ongoing Monitoring**.

Suspicious activity reporting

VII.201 The suspicious activity reporting requirements for RFIs are governed primarily by

Sections 43 through 48 of POCA, Sections 5 through 12 of ATFA, and POCR Regulations 16 and 17.

VII.202 RFIs conducting MSB must put in place appropriate policies and procedures to ensure that knowledge, suspicion and reasonable grounds for suspicion that funds or assets are criminal property or that a person is involved in ML/TF are identified, enquired into, documented and promptly reported.

VII.203 The definitions of knowledge, suspicion and reasonable grounds for suspicion are set forth in paragraphs 9.7 through 9.13 of the general GN.

VII.204 Many customers will, for perfectly good reasons, have an erratic pattern of transactions or activity. A transaction or activity that is identified as unusual, therefore, should not be automatically considered suspicious or as providing reasonable grounds for suspicion but should cause the RFI to conduct further, objective enquiries to determine whether the transaction or conduct is indeed suspicious or provides reasonable grounds for suspicion.

VII.205 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 and the identity of the persons who initiate or benefit from the transaction and/or conduct.

VII.206 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 criminal property or that a person is involved in ML/TF.

VII.207 In many circumstances, for purposes of reporting knowledge, suspicion or reasonable grounds for suspicion, an agent will be an RFI's employee and, therefore, must report to the RFI's reporting officer. In addition, where an RFI has knowledge, suspicion or reasonable grounds for suspicion concerning one of its agents, the RFI must also report such knowledge, suspicion or reasonable grounds for suspicion to the reporting officer.

VII.208 An RFI's reporting officer must consider each report, considering 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.

VII.209 Where, after evaluating an internal suspicious activity report, 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 suspicious activity report with the FIA.

VII.210 The FIA no longer accepts manually submitted suspicious activity reports (including those faxed or emailed). The FIA accepts only those suspicious activity reports submitted electronically via the goAML system, which is available at **www.fia.bm**.

VII.211 Where a reporting officer considers 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 suspicious activity report.

VII.212 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.

Failure to report and tipping-off offences

VII.213 Where an employee, including in many circumstances an agent, 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.

VII.214 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.

VII.215 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.

VII.216 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 the regulations or any direction or licence condition imposed by the BMA.

VII.217 Section 47 of POCA and Section 10A of ATFA contain tipping-off offences.

VII.218 It is a tipping-off offence under Section 47 of POCA and Section 10 of ATFA 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) Information or any other matter likely to prejudice any investigation that might be conducted following such a disclosure.

VII.219 It is also a tipping-off 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 person information or any other matter likely to prejudice the actual or proposed investigation.

VII.220 Any RFI investigation into a customer or a customer's activities, and any approach to the customer or to an introducing intermediary should be made with due regard to the risk of committing a tipping-off offence. See paragraphs 9.82 through 9.88 of the general GN.

VII.221 Detailed information on suspicious activity reporting, including related offences and constructive trusts, is set forth in **Chapter 9: Suspicious Activity Reporting**.

Employee and agent training and awareness

VII.222 The responsibilities of RFIs to ensure appropriate employee training and awareness are governed primarily by POCR Regulations 16 and 18.

VII.223 RFIs must take appropriate measures to ensure that relevant employees and agents:

a) Are aware of the acts and regulations relating to ML/TF;
b) Undergo periodic training on how to identify transactions or conduct that may be related to ML/TF; and
c) Know how to properly report knowledge, suspicion and reasonable grounds for suspicion that a transaction or conduct may be related to ML/TF.

VII.224 Each RFI must also ensure that relevant employees and agents 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 controls;
f) International sanctions (see paragraphs 6.52 through 6.54 of the general GN).

VII.225 In an MSB context, training should enable relevant employees and agents to:

a) Effectively vet both customers and the persons who own them, control them and act on their behalf;
b) Identify falsified documents;
c) Assess the risks associated with a customer and its transactions and/or business relationship with the RFI;
d) Conduct ongoing monitoring of the customer and its transactions and/or business relationship with the RFI; and
e) Recognise and report transactions or conduct where there is knowledge, suspicion or reasonable grounds for suspicion of ML/TF.

VII.226 Where an employee or agent exercises discretion for or in relation to a customer, the RFI must ensure that the employee or agent has an appropriate level of knowledge and experience to exercise the discretion properly, in accordance with the duties and obligations arising under the acts and regulations. Training may supplement the requisite level of knowledge and experience but likely cannot adequately replace it.

VII.227 RFIs should recognise that, often, multiple ML/TF typologies and techniques are used in a single transaction or in a series of related transactions. RFIs should, therefore, be alert to indicators of potentially suspicious transactions from all categories of typology or technique. RFIs should also incorporate the regular review of ML/TF trends and typologies into their employment and agent screening and compliance training programmes, as well as into their risk identification and assessment procedures. Information on trends, typologies and techniques is available from a wide variety of publicly available sources, including but not limited to FATF and CFATF publications.

VII.228 Detailed information on employee training and awareness is set forth in **Chapter 10: Employee Training and Awareness**.

Record-keeping

VII.229 The record-keeping obligations of RFIs are governed primarily by POCR Regulations 15 and 16.

VII.230 Under POCR Regulation 16(4), each RFI must have systems in place enabling it to respond promptly to enquiries from a supervisory authority, the FIA or a police officer, about whether the RFI maintains, or has maintained during the previous five years, a business relationship with any person, and the nature of that relationship.

VII.231 RFIs must keep specified records for a period of at least five years following the date on which the business relationship ends or, in the case of an occasional transaction, following the date on which the transaction, or the last in a series of transactions, is completed.

VII.232 RFIs conducting MSB should ensure the monitoring systems the RFI uses are

searchable and record historical transactions.

VII.233 Detailed information on the records that must be kept is set forth in **Chapter 11: Record-Keeping**.

MSBs as customers of other RFIs

VII.234 In many instances, MSBs are reliant on access to banking and other financial services to commence or continue their operations. It is important that RFIs apply the risk-based approach properly to any proposed or existing business relationship with an MSB.

VII.235 RFIs should not resort to the wholesale termination or exclusion of business relationships with MSBs without first being informed by a proper risk assessment. Some financial institutions, perceiving MSBs to be high risk for ML/TF, for the reasons set forth in paragraph VII.64, have categorically terminated business relationships with MSBs and refused to accept MSBs as new customers. Such a systematic rejection of MSBs as customers risks driving classes of legitimate customers to transact outside of the regulated financial sector or may cause classes of legitimate customers to be unable to access the service in question through any means.

VII.236 Where an RFI reviewing a proposed or existing business relationship with an MSB determines, based on a thorough review of available information, that the business relationship is or would be higher risk, the RFI should evaluate whether the risks identified can be appropriately mitigated and managed. RFIs are not required to eliminate risk entirely; they are required to effectively mitigate and manage risk, for example, by applying enhanced due diligence measures commensurate with the risks the RFI properly assesses, that are designed to obtain additional information about the MSB, its owners, agents, policies and procedures, operations and customers.

VII.237 RFIs should consider the degree to which an MSB is subject to licensing or registration requirements and effective supervision for AML/ATF purposes and the degree to which such licensing, registration and/or effective supervision serves to mitigate any of the risks the RFI identifies in connection with the MSB. RFIs should take note that under Bermudian law, Bermudian MSBs are RFIs subject to POCA, ATFA, POCA SEA, POCR and these guidance notes, and are supervised by the BMA.

VII.238 RFIs evaluating the commencement or continuation of a business relationship with an MSB customer may consider enquiring into the items below as part of the RFI's risk assessment of the business relationship and/or as part of any enhanced due diligence measures applied to mitigate and manage risks:

a) Whether the business is properly licensed, registered and regulated;
b) Whether the business is registered in and operates from an equivalent

jurisdiction;
c) Whether the business is a principal in its own right or an agent of another principal;
d) The length of time the business has operated;
e) The identity, experience and reputation of the business' beneficial owners and managers;
f) The business' formal AML/ATF policy statement (see paragraphs 1.31 through 1.37 of the general GN)
g) The business' AML/ATF policies, procedures and controls, including group-wide compliance programmes;
h) The names and contact information for the business' compliance officer and reporting officer (see paragraphs 1.38 through 1.50 of the general GN);
i) The business' internal and/or independent audits of the functioning of its AML/ATF policies, procedures and controls (see paragraphs 1.78 through 1.85 of the general GN);
j) The business' policies, procedures and controls for screening, on-boarding, training and overseeing employees and agents;
k) The business' agent list;
l) The business' client profile;
m) The business' products and services profile;
n) The purpose of the MSB's proposed account(s) or business relationship and the type and level of anticipated account or other business activity; and
o) The business' assessment of the ML/TF risks it faces and the mitigating measures it has put in place.

VII.239 MSBs seeking to commence or continue a business relationship with another RFI should be prepared to provide that other RFI, upon request, with information about the items in paragraph VII.238 to ensure that the other RFI is able to meet its regulatory obligations and provide financial services to the MSB.

Risk factors for MSB

VII.240 In addition to the non-exhaustive list of risk factors set forth in paragraph 2.37, RFIs conducting MSB should consider sector-specific risk factors, including those in paragraphs VII.241 through VII.246 below, in order to fully assess the ML/TF risks associated with a particular business relationship. The non-exhaustive list of sector-specific risk factors addresses customers and business relationships, countries and geographic areas, products and services, transactions, delivery channels and third-party service providers.

VII.241 Customer and business relationship risk factors include, but are not limited to:

a) A customer who offers false, fraudulent, fictitious or expired identification information or documents;
b) Unjustified delays in the production of identity documents or other requested information;
c) A non-face-to-face customer, where doubt exists about the identity of the

customer;

d) A customer who knows little or is reluctant to disclose basic details about the payee;
e) A customer who has only vague knowledge about the amount of money involved in the transaction;
f) A customer who gives inconsistent information;
g) A customer transacting with a jurisdiction with which the customer has no apparent ties;
h) A customer who appears to be acting on behalf of a third party but does not disclose that information;
i) One or more persons other than the customer, watching over the customer or waiting just outside of the RFI;
j) A customer reading from a note or mobile phone while providing details of the transaction;
k) A customer who appears to be nervous or creating a sense of extreme urgency;
l) A customer travelling unexplained distances to different locations of the RFI and/or its agents to conduct transactions;
m) A customer who owns or operates a cash-based business;
n) The involvement of any PEP as a person owning, controlling or representing the customer, or as a person otherwise connected with the customer;
o) A customer who is known to the RFI to have been the subject of law enforcement sanctions in relation to crime generating proceeds;
p) A customer who begins a transaction but cancels the transaction after learning of a CDD requirement;
q) A customer who threatens or tries to convince the RFI's personnel to avoid reporting;
r) A customer who is a member of a class of persons considered higher risk for ML/TF;
s) The unnecessary granting of a power of attorney;
t) A customer who is unwilling or unable to provide satisfactory information to verify the source of wealth or source of funds;
u) Levels of assets or transactions that exceed what a reasonable person would expect of a customer with a similar profile;
v) A customer offering to pay extraordinary fees for unusual services or for services that would not ordinarily warrant such a premium;
w) Requests for payment to be made via the RFI's client money account, where such a payment would normally be made from a customer's own account;
x) Requests for anonymity that go beyond a reasonable request for discretion;
y) A customer or counterparty that is another MSB or financial institution that a respective national competent authority has sanctioned for non-compliance with applicable AML/ATF regulations and that is not engaging in remediation to improve its compliance;
z) A customer who uses agents or associates such that it is difficult for the RFI to identify the beneficial owner of the funds; and
aa) A transaction or business relationship that uses complex networks of legal arrangements where there is no apparent rationale for the complexity or where the complexity appears to be intended to conceal the true ownership or control

arrangements from the RFI.

VII.242 Country and geographic area risk factors include, but are not limited to:

a) A customer, person acting on behalf of the customer, person owning or controlling the customer or any agent or other third party associated with the customer who is a resident in, or citizen of, a high-risk jurisdiction;
b) An MSB transaction to, through or from a high-risk jurisdiction;
c) A non-face-to-face transaction initiated from a high-risk jurisdiction;
d) An MSB transaction linked to business in or through a high-risk jurisdiction;
e) MSB involving persons or transactions with a material connection to a jurisdiction, entity, person or activity that is a target of an applicable international sanction; and
f) An MSB relationship or transaction for which an RFI's ability to conduct full CDD may be impeded by another jurisdiction's confidentiality, secrecy, privacy or data protection restrictions.

VII.243 Products and services risk factors include, but are not limited to:

a) Products or services that may inherently favour anonymity;
b) Products that can readily cross international borders, such as cash, online money transfers, stored value cards, money orders and international money transfers by mobile phone or the internet;
c) Products or services that have a very high or no transaction limit;
d) Products or services that permit the exchange of cash for a negotiable instrument, such as a stored value card or a money order; and
e) Other products or services that are addressed in paragraphs 5.36 through 5.93 of the general GN.

VII.244 Transaction risk factors include, but are not limited to:

a) Transactions that are just below the RFI's thresholds for due diligence checks;
b) Transactions that appear to have no obvious economic or financial basis;
c) Unusual, complex or uncharacteristically large transactions;
d) Transactions that route through third countries or third parties;
e) Transactions accompanied by information that appears false or contradictory;
f) A wire transfer or money transmission that is not accompanied by all required information;
g) A transaction to a country or region that is outside of the RFI's normal business;
h) Cashing third-party cheques endorsed to the customer;
i) Cashing checks from financial institutions in jurisdictions that pose a higher risk for ML/TF or from countries identified as having weak AML/ATF controls;
j) Large cash or bearer instrument transactions in circumstances where such a transaction would normally be made by cheque, banker's draft or wire transfer;

k) Transfers to the same person from different individuals or to different persons from the same individual with no reasonable explanation;
l) Transfers of funds that are not in line with the stated business activities of the customer;
m) Customers requesting transfers to or from overseas locations with instructions for payment to be made in cash;
n) Transactions from another MSB that is not acting as the RFI's agent;
o) Transactions of a size or volume that exceeds what a reasonable person would expect of a customer with a similar profile, or given the nature and stated purpose of the transaction or business relationship;
p) One-off transactions giving rise to suspicion; and
q) Requests for funds, shares or other assets to be transferred to PEPs or higher-risk charities or other not-for-profit organisations not subject to effective supervision and monitoring.

VII.245 Delivery channel risk factors include, but are not limited to:

a) A lack of face-to-face contact with the customer and any persons associated with them;
b) Any request to carry out significant transactions using cash, or using any payment or value transfer method that obscures the identity of any of the parties to the transaction; and
c) The use of third-party intermediaries, agents or brokers.

VII.246 Agent and third party risk factors include, but are not limited to:

a) The involvement of any agent or third party in carrying out any AML/ATF function in relation to a customer, including reliance upon, or outsourcing to, any agent or third party that has not been sufficiently reviewed for compliance with paragraphs 5.117 through 5.148 (reliance) and 5.149 through 5.174 (outsourcing) of the general GN. This includes any involvement of an agent or third party that would:
    i. Impede 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;
    ii. Impede the effective ability of the RFI's board or similarly empowered body or natural person to provide oversight;
    Impede the effective ability of the appropriate regulator to monitor the RFI's compliance with all obligations under the regulatory system;
    iii. Reduce the responsibility of the RFI and/or its managers and officers;
    iv. Remove or modify any conditions subject to which the RFI's authorisation was granted; or
    v. Increase ML/TF risk in any way that is not adequately addressed through appropriate risk assessment and mitigation;
b) Agents for which the RFI is unable to satisfactorily complete the steps set forth in paragraph VII.166;
c) Agents that refuse to provide information requested for inclusion in the RFI's

agent list;

d) Agents representing more than one RFI;
e) An agent that has its own agents for which it provides inadequate supervision;
f) Agents located in a higher-risk jurisdiction or serving higher-risk customers or transactions;
g) Agents that are, or involve, PEPs;
h) Agents conducting an unusually high number of transactions with another agent location, particularly with an agent in a higher-risk geographic area or corridor;
i) Agents that have transaction volume that is inconsistent with either overall transaction volume or relative to typical past transaction volume;
j) Agents that have been the subject of negative attention from credible media or law enforcement sanctions;
k) Agents that have failed to attend or satisfactorily complete the RFI's training programmes;
l) Agents that do not effectively manage compliance with the RFI's AML/ATF policies, procedures and controls;
m) Agents that fail to provide required originator information upon request.

***