# Annex VI

# Sector-Specific Guidance Notes (SSGN) for Corporate Service Provider (CSP) Business

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

# Table of Contents

## ANNEX VI

## SECTOR-SPECIFIC GUIDANCE NOTES FOR CORPORATE SERVICE PROVIDER BUSINESS

### *Introduction*

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

VI.2 Under Section 42A(1)(fa) of the Proceeds of Crime Act 1997 (POCA), persons carrying on CSP business within the meaning of the Corporate Service Provider Business Act 2012 are designated as AML/ATF Regulated Financial Institutions (RFI).

VI.3 Under Section 2(2) of the Corporate Service Provider Business Act 2012, CSP business means the provision of any of the following corporate services for profit:

a) Acting as a company formation agent or agent for the establishment of a partnership;
b) Providing nominee services, including (without limitation) acting as or providing nominee shareholders;
c) Providing administrative and secretarial services to companies or partnerships, including one or more of the following services:
    i. Providing a registered office;
    ii. Providing an accommodation, correspondence or administrative address;
    iii. Maintaining the books and records of a company or partnership;
    iv. Filing statutory forms, resolutions, returns and notices;
    v. Acting as or fulfilling the function of, or arranging for another person to act as or fulfil the function of, a person authorised to accept service of process on behalf of a company or partnership or to accept any notices required to be served on it;
    vi. Acting as or fulfilling the function of, or arranging for another person to act as or fulfil the function of, a director, officer, secretary, alternate, assistant or deputy secretary of a company or an officer of a partnership;
    vii. Keeping or making any necessary alterations in the register of members of a company in accordance with Section 65 of the Companies Act 1981;
d) The performance of functions in the capacity of resident representative under the Companies Act 1981, Exempted Partnerships Act 1992 and the Overseas Partnerships Act 1995; and
e) Providing any additional corporate or administrative services as may be specified in regulations.

VI.4 The references in paragraph VI.3 to companies and partnerships are to companies and partnerships wherever they are incorporated or otherwise established and to any similar or equivalent structures or arrangements; however, they are named.

VI.5 All RFIs must comply with the acts and regulations and with the general

AML/ATF GN issued by the Bermuda Monetary Authority (Authority or BMA).

VI.6 Schedule 1, Section 3(2) of the Corporate Service Provider Business Act 2012, as amended in 2019, states that in determining whether a CSP is conducting its business in a prudent manner, the BMA will take into account any failure to comply, among other things, with:

a) The POCA;
b) The Anti-Terrorism (Financial and Other Measures) Act 2004 (ATFA);
c) The Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 (POCR);
d) The Corporate Service Provider Business Act 2012;
e) Relevant codes of practice issued by the BMA; and
f) International sanctions in effect in Bermuda.

VI.7 For the purposes of these SSGN, the terms AML/ATF regulated financial institution and RFI should be understood to include persons conducting the CSP business described in paragraph VI.3. CSP business should be understood to include any and all of the activities described in paragraph VI.3.

VI.8 RFIs conducting CSP business should read these SSGN in conjunction with the general GN. This annex supplements, but does not replace, the general GN.

VI.9 Portions of this annex summarise or cross-reference relevant information that is contained in detail in the general GN. Nevertheless, the detailed information in the GN remains the authoritative guidance.

VI.10 Portions of this annex include sector-specific information, such as risk indicators that are particular to CSP business. This sector-specific information should be considered supplementary to the general GN.

***Status of the Guidance***

VI.11 Pursuant to Section 49M of POCA and 12O of ATFA, these SSGN are issued by the BMA under Section 5(2) of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 (POCA SEA), approved by the Minister of Legal Affairs and available for download on the website of the BMA at www.bma.bm.

VI.12 These SSGN 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 and Terrorist Financing (ML/TF).

VI.13 The Supreme Court (Court), or the BMA, as the case may be, in determining whether a person is in breach of a relevant provision of the acts or regulations, is

required to consider whether a person has followed any relevant guidance approved by the Minister of Legal Affairs and 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 12O of, and paragraph 1(6) of Part I, Schedule I of the ATFA and Section 20(6) of the POCA SEA.

VI.14 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.

VI.15 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.

VI.16 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.

VI.17 RFIs should be aware that under Section 16(1) of the Financial Intelligence Agency Act 2007, the Financial Intelligence Agency (FIA) may, in the course of enquiring into a suspicious transaction or activity relating to ML or 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.

VI.18 Detailed information is set forth in the general GN, beginning with the **Preface**.

***Senior Management Responsibilities and Internal Controls***

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

VI.20 The AML/ATF internal control requirements for RFIs conducting CSP business are governed primarily by Part 3 of the POCR.

VI.21 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.

VI.22 Section 20 of the POCA SEA empowers the BMA to impose a penalty on any person supervised by the BMA in an amount up to $10 million for each failure to comply with specified regulations. The POCA SEA also provides for a number of criminal offences, including carrying on business without being registered pursuant to Section 9 of the Corporate Service Provider Business Act 2012.

VI.23 Senior management of 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.

VI.24 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 inquiries and inspections by competent authorities, including but not limited to sample testing of customer files; and
l) Recognise potential personal liability if legal obligations are not met.

VI.25 RFIs must establish and maintain detailed policies, procedures and controls that are adequate and appropriate to forestall and prevent operations related to ML/TF.

VI.26 RFIs should consider using proven technology-driven solutions to minimise the risk of error and find efficiencies in their AML/ATF processes.

VI.27 Under Section 10(2)(c) of the Corporate Service Provider Business Act 2012, an RFI must include its AML/ATF policies and procedures with its application for a CSP business licence. RFIs should also submit a business risk assessment and client risk assessment at the time of application.

VI.28 Where a Bermuda RFI conducting CSP business has branches, subsidiaries, representative offices or members of any financial group located in a country or territory other than Bermuda, it must communicate its AML/ATF policies and procedures to all such entities. It must ensure that all such entities apply AML/ATF measures at least equivalent to those set out in the acts and

regulations.

VI.29 Attempts to launder money through CSP business services 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 or employee, either individually or in collusion with others inside and/or outside the RFI conducting CSP business; 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.

VI.30 The majority of this annex addresses attempted ML by customers. ML risks involving third parties are addressed in paragraphs VI.123 through VI.128. ML risks involving internal senior management, directors, managers or employees are addressed primarily via fit and proper requirements for CSPs and in paragraphs VI.36 through VI.39.

VI.31 Specific requirements for an RFI's detailed policies, procedures and controls are set forth in **Chapters 2 through 11** of the general GN.

VI.32 Detailed information is set forth in **Chapter 1: Senior Management Responsibilities and Internal Controls**.

Links between CSP business practices and AML/ATF policies, procedures and controls.

VI.33 Persons carrying on CSP business 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:

a) Limited Partnership Act 1883;
b) Exchange Control Regulations 1973;
c) Companies Act 1981;
d) Exempted Partnerships Act 1992;
e) Overseas Partnerships Act 1995;
f) Corporate Service Provider Business Act 2012; and
g) Limited Liability Company Act 2016.

VI.34 Persons carrying on CSP business may also be subject to the requirements, principles, standards and procedures set forth in guidance documents. These guidance documents for CSPs include, but are not limited to:

a) Statement of Principles (BMA – December 2019) made pursuant to Section 6 of the Corporate Service Provider Business Act 2012;
b) Code of Practice (BMA – December 2019) made pursuant to Section 7 of the

Corporate Service Provider Business Act 2012;
c) Guidance Notes (BMA – March 2020);
d) Corporate Governance Policy (BMA – February 2016); and
e) Further Guidance (BMA – June 2017).

VI.35 The requirements of the acts, regulations and additional guidance documents described in paragraphs VI.33 through VI.34 provide a suitable foundation for the AML/ATF policies, procedures and controls that Bermuda RFIs are required to adopt and implement. An RFI should not presume, however, that its existing processes are sufficient. Each RFI must ensure that it meets each of its AML/ATF obligations under the Bermuda acts, regulations and these SSGN, whether as part of its existing business processes or through separate processes.

Ownership, management and employee checks

VI.36 To guard against potential ML involving owners, directors, managers and employees of CSPs, Regulation 18(1)(c) requires RFIs conducting CSP business 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, and in the Further Guidance (June 2017) described in paragraph VI.34.

VI.37 RFIs should ensure that screenings are conducted both for the RFI itself and for any intermediary or third-party service provider.

VI.38 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.

VI.39 Working with 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 CSP business will need to undertake in order to meet its screening obligations.

***Monitoring and Managing Compliance***

VI.40 RFIs must appoint a compliance officer, who must be at the managerial level, who is appropriately qualified and trained and who 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.

VI.41 RFIs must also appoint a reporting officer, who under the RFI's policies and procedures:

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

VI.42 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 is in compliance 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 for RFIs Conducting CSP Business***

VI.43 As described in **Chapter 2: Risk-Based Approach**, RFIs, including CSPs, 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, CSPs 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 to which the CSP is exposed, 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 Caribbean Financial Action Task Force (CFATF) and Financial Action Task Force (FATF); and
e) The internal audit function and regulatory findings.

VI.44 The 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 future national risk assessments.

VI.45 RFIs should document and be in a position to justify the basis on which they have assessed the level of risk associated with each particular combination of customer, business relationship, country or geographic area, service, delivery channel, product or transaction.

VI.46 When designing and evaluating a new product or service, an RFI conducting CSP business must, prior to launch, assess the risk of the product or service being used for ML/TF.

VI.47 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.

VI.48 RFIs conducting CSP business must employ a risk-based approach in determining:

a) Appropriate levels of Customer Due Diligence (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.

VI.49 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.

VI.50 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.

VI.51 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.

VI.52 RFIs conducting CSP business are gatekeepers who, in addition to serving the interests of their customers, serve the broader interests of the public. 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.

VI.53 Legal persons, including corporates, vary greatly in terms of size, complexity, activities undertaken and the degree to which their control and ownership structures are transparent. Corporates listed on an appointed stock exchange tend to be larger, more complex and, due to their public ownership, more transparent. Privately held corporates may be of a range of sizes and complexity but tend to be less transparent.

VI.54 Regardless of a particular legal entity's features, RFIs must use a risk-based approach to determine whether there are legitimate commercial purposes for the

size, structure and level of transparency of each customer and whether the customer or business relationship entails a heightened level of ML/TF risk.

VI.55 Although RFIs conducting CSP business 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.

VI.56 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**.

VI.57 Using the risk-based approach, each RFI conducting CSP business should determine its risk tolerance, which is the amount of ML/TF risk the RFI will accept in pursuit of its business goals.

VI.58 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.

VI.59 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.

VI.60 Corporate services are used more frequently for the layering stage of ML than for the initial placement of criminally involved funds. Criminals seeking to launder money with the involvement of a CSP business are attracted primarily by:

a) Business structures that obscure the identity of the private natural persons who own and control the entity;
b) The ability to conceal or disguise the illicit origin of funds;
c) The potential to transfer or exact value or utility from the assets involved in a business structure for the benefit of criminals;
d) The possibility of legally relocating assets from one jurisdiction to another; and
e) The use of CSPs (gatekeepers) as nominee directors and shareholders to hide the ownership and control of assets.

VI.61 The level of risk associated with CSP business depends in part on the services the RFI provides. The level of risk is generally higher where:

a) The RFI is involved in the management of a customer's financial affairs;
b) A customer has a complex structure or legal arrangement;
c) A customer's beneficial owners change frequently and/or without timely notice to the RFI where requested;
d) A customer has multiple accounts and/or is engaged in complicated transfers and transactions;
e) A customer uses third-party intermediaries, proxies or legal entities or arrangements, which can separate the source of funds from the transaction or activity being carried out; or
f) A customer's business involves legal entities formed or registered under foreign law such that the ownership and control structure of each entity is not readily understood.

VI.62 For example, the risks faced by an RFI acting as a company director involved in the management of a customer's financial affairs will be significantly higher than the risks faced by an RFI that merely administers the identification and appointment of directors who are not employed by the RFI.

VI.63 RFIs should evaluate and consider obtaining legal advice on the level of responsibility that may be imputed to the RFI due to a customer's actions, including but not limited to the following circumstances:

a) Where an RFI provides registered office or registered agent services but does not have direct control over the customer legal entity;
b) Where an RFI supplies directors to a customer with a split board arrangement; and
c) Where a customer requests any mail holding arrangement or care of (c/o) mail arrangement.

VI.64 Where a customer requests any mail holding arrangement or care of (c/o) mail arrangement, the RFI should obtain the reasons for and details of the arrangement, conduct enhanced monitoring and consider whether this deliberate request is meant to obscure who ultimately owns and controls the company. The RFI should also consider what other action is required due to the higher risk of ML/TF, consider business termination and consider filing a suspicious activity report depending on the circumstances.

VI.65 Specific indicators of higher risk in CSP business are discussed in detail in paragraphs VI.204 through VI.210 of this annex.

***Customer Due Diligence***

VI.66 RFIs conducting CSP business must carry out CDD.

VI.67 Detailed information on CDD is set forth in **Chapters 3, 4 and 5** of the general GN, and paragraphs VI.66 through VI.148 of this annex.

VI.68 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 by providing information on CSP customers or activities being investigated.

VI.69 CDD measures that must be carried out include:

a) Identifying and 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 at the customer; and
h) Updating the CDD information at appropriate times, including 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.

VI.70 Under Section 4(a) of the BMA's Further Guidance for CSPs (June 2017), all vetting, which may include verifications of CDD information, should be carried out using two search engines, independent of each other.

VI.71 Detailed information on CDD for legal persons and other legal arrangements is set forth in paragraphs 4.61 through 4.136 and Annex I.

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

VI.72 An RFI must understand the nature of the customer's business and the purpose and intended nature of each proposed business relationship or transaction. In

some instances, the nature of the customer's business and the purpose and intended nature of a proposed business relationship may appear self-evident. Nonetheless, an RFI must obtain information that enables it to categorise the customer's business and the nature, purpose, size and complexity of the business relationship so that it can be effectively monitored.

VI.73 An RFI should obtain sufficient information to reasonably satisfy that there is a legal, commercial or personal rationale for the CSP work being undertaken.

VI.74 To obtain an understanding sufficient to monitor a CSP business relationship or transaction, an RFI should collect information, including but not limited to:

a) The customer's goals for the CSP business relationship or transaction;
b) The source of wealth and source of funds to be used in the CSP business relationship or transaction;
c) The anticipated type, volume, value, frequency, duration and nature of the activity that is likely to be undertaken through the CSP business relationship or transaction;
d) The geographic connections of the customer and each beneficial owner, administrator, advisor, operator, employee, manager, director or other person who can exercise significant power over the CSP business relationship or occasional transaction;
e) The means of payment (cash, wire transfer, other means of payment);
f) Whether there is any 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.

Source of wealth and source of funds

VI.75 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.

VI.76 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 CSP business relationship or transaction.

VI.77 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.

VI.78 RFIs should also ensure they understand the source of funds and specific means of payment, including the details of any account a customer proposes to use.

VI.79 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 a CSP business context

VI.80 An RFI's customer is generally a private natural person, legal person, trust or other legal arrangement with and for whom a business relationship is established, or with or for whom an occasional transaction is carried out. A given CSP business relationship or transaction may have more than one person who is a customer.

VI.81 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.

VI.82 For the purposes of these SSGN, 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 a CSP business product or service; and
b) Each beneficial owner of a customer.

VI.83 Where, for example, a company approaches a CSP to identify a suitable director, and the director who is placed with the company pays the CSP for assistance in securing the placement, then the company, its beneficial owners and the director identified by the CSP are customers of the CSP.

VI.84 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 Customer Due Diligence Measures**.

Definition of 'beneficial owner' in a CSP business context

VI.85 Irrespective of a customer's geographic location, 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.

VI.86 Under Regulation 3(11), CSP businesses must consider as beneficial owners any persons, whether private natural persons, legal persons or legal arrangements, that effectively own or control more than 10% of a customer's funds, assets or voting rights, or in the case of trusts or similar legal arrangements. The meaning of 'control' and 'own' in this context should be interpreted broadly to comprise the capacity to:

a) Manage funds, assets, accounts or investments without requiring further

authorisation;
b) Direct management to take or refrain from taking an action;
c) Override internal procedures and control mechanisms;
d) Derive benefit, whether presently or in the future;
e) Exercise a specified interest, whether presently or in the future; and/or
f) Add or remove beneficiaries, trustees, signatories, nominees or other persons associated with a customer, including but not limited to directors, secretaries, partners, general partners or members.

VI.87 Where another legal person or legal arrangement holds control or ownership, RFIs should consider as a beneficial owner each private natural person who ultimately controls or owns that other legal person or legal arrangement.

VI.88 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.

VI.89 Information on the identification and verification of beneficial owners is set forth in Regulation 3 and **Chapter 4: Standard Customer Due Diligence Measures**.

VI.90 Additional information specific to the beneficial ownership of trusts is set forth in Regulation 3(3) and paragraphs I.78 through I.87. Information specific to control over trust is set forth in Regulation 3(4) and paragraphs I.65 through I.70.

Obtaining and verifying customer identification information

VI.91 RFIs must obtain and verify identification information for each person who is a customer in the CSP business context.

VI.92 A person who is a customer in the CSP business context may be a natural person, legal person, trust or other legal arrangement. For each type of customer, RFIs should follow the identification and verification requirements in **Chapter 4: Standard Customer Due Diligence Measures**, as supplemented by any relevant Annexes.

VI.93 In addition to the information required for all customers, RFIs must obtain the following identification information in relation to each corporate customer:

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

j) Control and ownership (see paragraphs 4.75 through 4.96).

VI.94 RFIs must verify the following in relation to each corporate customer:

a) Full name;
b) Date and place of incorporation, registration or establishment;
c) Official identification number (where applicable);
d) Current existence of the corporate; and
e) The legal powers that regulate and bind the customer.

VI.95 Partnerships that are legal persons should be identified and verified using the guidance for legal persons set forth in paragraphs 4.75 through 4.96. In such cases, for verification, RFIs may obtain sight of and retain a record of the following documents in lieu of or in addition to a certificate of incorporation, articles of association or equivalent constitutional documentation:

a) Partnership agreement; and/or
b) Registered business name certificate.

VI.96 Where a customer is an unincorporated partnership or business, the RFI must determine whether to treat as customers the persons owning and controlling the partnership or business, the underlying business or both.

VI.97 The RFI should verify the existence, ownership and control structure of a corporate by:

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

VI.98 Examples of measures an RFI can take to verify the nature of a customer's business include, but are not limited to:

a) Confirming a customer's internet presence, including browsing and retaining a record of a customer's web page;
b) Obtaining confirmations from reliable third parties familiar with the customer and its business;
c) Conducting a site visit to the customer's place of business; and
d) Making telephone or internet inquiries to the company to confirm the products and services it offers.

VI.99 Regardless of the method(s) used, all required information must be verified.

VI.100 Where an RFI is unable to complete verification using the methods contained in paragraph VI.97, where the size or complexity of a corporate is significant, where the ownership or control structure of a customer is unclear, or where a business relationship is otherwise assessed as higher risk, the RFI should consider the extent to which additional evidence is required. Additional means of verification may include:

a) Reviewing an independently audited copy of the latest report and accounts;
b) Reviewing a copy of the director or shareholder's register;
c) Reviewing the board resolution authorising the transaction or business relationship and recording signatories;
d) Reviewing the ownership and control structure of any group of which the customer is part;
e) Engaging a business information service or a reputable and known firm of lawyers or accountants to confirm the documents submitted;
f) Utilising independent electronic databases; and
g) Personally visiting the principal place of business.

VI.101 Where the customer is an unincorporated partnership or business, RFIs must verify the following:

a) Full name;
b) Business address;
c) Official identification number (where applicable);
d) Current existence of the customer;
e) Ownership and control structure of the customer;
f) The legal powers that regulate and bind the customer;
g) Subject to paragraphs VI.108 and VI.109, the identity of all partners, principals, members, directors and other persons exercising control over the management of the unincorporated partnership or business;
h) The identity of at least a natural person holding the position of chief executive or a person or equivalent or similar position; and
i) The identity of all other persons purporting to act on behalf of the customer or by whom binding obligation may be imposed on the customer.

VI.102 Full information on identifying and verifying partnership customers is set forth in **Chapter 4: Standard Customer Due Diligence Measures**.

VI.103 Full information on identifying and verifying trust customers is set forth in **Chapter 4: Standard Customer Due Diligence Measures** and in Annex I.

Obtaining and verifying beneficial owner information

VI.104 RFIs conducting CSP business must obtain identification information in line with the guidance for private persons and, where relevant, legal persons for the natural

persons who ultimately own and control any customer that is a legal person, trust or other legal arrangement, including, but not limited to:

a) All directors, signatories and other persons exercising control over the management of the corporate;
b) All private natural persons who, either directly or indirectly via one or more other natural persons, legal persons or legal arrangements, ultimately control or own more than 10% of a customer's funds, shares, assets or voting rights or interest;
c) At least one natural person holding the position of chief executive or a person of equivalent or similar position; and
d) All other persons purporting to act on behalf of the corporate or by whom a binding obligation may be imposed on the corporate.

VI.105 A limited exception to this fundamental rule may apply where a corporate customer's securities are listed on an appointed stock exchange. Additional information on this exception is set forth in paragraphs 4.97 through 4.98 of the general GN.

VI.106 RFIs must verify the following in relation to each corporate customer:

a) The ownership and control structures of the corporate, to include in the case of multi-layered structures information sufficient to fully understand the entity's intermediate ownership and control structure;
b) At least one natural person holding the position of chief executive or a person of equivalent or similar position;
c) Subject to paragraphs VI.108 and VI.109, the identity of all directors, signatories and other persons exercising control over the management of the corporate; and
d) The identity of all other persons purporting to act on behalf of the corporate or by whom binding obligations may be imposed on the corporate.

VI.107 In addition, and on the basis of an assessment of the ML/TF risks associated with a customer and its business relationship, RFIs conducting CSP business must take reasonable measures to verify the identity of all private natural persons who, either directly or indirectly via one or more other natural persons, legal persons or legal arrangements, ultimately control or own more than 10% of a customer's funds, shares, assets or voting rights.

VI.108 Where the number of directors, partners, principals, members, signatories and other persons exercising control over the management of the corporate is high, RFIs may use a risk-based approach to determine whose identity to verify. Where ML/TF risks are standard or low, RFIs should verify at least two of the relevant signatories and, where different, two directors or other natural persons exercising significant control over the management of the customer. The natural persons verified should be those the RFI expects to hold signatory powers for the purpose of operating an account or exchanging instructions. Where the ML/TF risks are

higher or where a customer may be seeking to avoid the application of certain CDD measures, the RFI may find it necessary to verify all directors and other natural persons exercising significant control over the management of the customer. An RFI should not act on an instruction from a natural person whose identity the RFI has not verified.

VI.109 Where any natural person associated with the customer is assessed as higher risk, for example, where a Politically Exposed Person (PEP) or a target of international sanctions is involved, or where a business relationship is assessed as a higher risk for any reason, including but not limited to the involvement of a higher-risk jurisdiction, all signatories, directors and other natural persons exercising control over the management of the customer must be verified.

VI.110 An RFI conducting CSP business should ensure that agreements with customers:

a) Are maintained in writing;
b) Include a clear description of the services to be provided, fees to be charged, and the manner in which fees are expected to be deducted or paid; and
c) State how and by whom authorised requests for action are to be given.

VI.111 Where any customer has or is requesting a nominee service, the RFI must identify the nominator and seek to understand why any beneficial owner is seeking nominee services.

VI.112 Where an RFI provides or arranges for others to provide a nominee service, the RFI must ensure that the written nominee agreement identifies the nominator and beneficial owners and that the RFI retains a copy of the agreement in its records.

VI.113 Where a customer is an agent acting on behalf of a principal, 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.

VI.114 Full information on identifying and verifying partnership customers and the beneficial owners and persons exercising significant control over partnerships is set forth in paragraphs 4.124 through 4.130 of the general GN.

VI.115 Full information on identifying and verifying trust beneficiaries is outlined in **Chapter 4: Standard Customer Due Diligence Measures** and Annex I.

Timing of customer due diligence

VI.116 An RFI must apply CDD measures when it:

a) Establishes a business relationship;
b) Carries out an occasional transaction in an amount of $15,000 or more, whether the transaction is carried out in a single operation or several

operations which appear to be linked, or carries out any wire transfer in an amount of $1,000 or more (see **Chapter 8: Wire Transfers**);
c) Suspects ML/TF; or
d) Doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

VI.117 Where the product or service is a one-off transaction amounting to less than $15,000(e.g., company formation but no further services are required that would involve an ongoing business relationship with the customer), then, in line with the RFI's risk assessment, verification of identity may not be necessary.

VI.118 Nevertheless, where a customer who has carried out a one-off transaction amounting to less than $15,000 requests a future or ongoing service or returns to carry out further transactions, the RFI should consider entering into a business relationship requiring CDD measures.

VI.119 Without exception, RFIs conducting CSP business should always identify the customer, the relevant persons comprising the customer, beneficial owners, persons exercising significant control, the nature of the customer's business, the purpose and intended nature of the business relationship, and the source of wealth and source of funds before the establishment of a business relationship or the carrying out of an occasional transaction.

VI.120 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;
c) Before the RFI allows the exercise of any power or control;
d) When a new party becomes entitled to exercise power or control; and
e) 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.

VI.121 Each time a new or existing customer adds assets to any customer portfolio managed or overseen by an RFI, the RFI should obtain and verify the source of the assets and the objectives of the customer.

VI.122 Detailed information on the timing of CDD measures is set forth in **Chapter 3: Overview of Customer Due Diligence**.

<u>Previous due diligence and reliance on third parties</u>

VI.123 Paragraphs 5.117 through 5.148 set forth the circumstances in which reliance on a third party is permissible. Paragraphs 3.23 through 3.25 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.

VI.124 Before an RFI conducting corporate service business can rely on CDD conducted by a third party, the RFI must determine whether the third party carried out at least the standard level of customer verification.

VI.125 RFIs may rely upon another person or institution to carry out CDD measures only when the person or institution being relied upon confirms in writing that the measures have actually been applied. A Bermudian RFI or a non-Bermudian entity conducting business corresponding to the business of a Bermudian RFI that has relied upon another person to apply certain CDD measures may not 'pass on' verification to a third institution.

VI.126 An RFI that is taking over from a previous CSP or acting as an additional CSP should obtain a sight of and retain record of all original due diligence documentation.

VI.127 Where an RFI determines that the information it has received is adequate and all other criteria for relying upon a third party have been met, the RFI may determine that it has satisfied its CDD obligations.

VI.128 Where, nonetheless, an RFI determines that relevant documentation is not available or is inadequate, the RFI must seek additional documentation.

Refusing or terminating CSP business

VI.129 If for any reason an RFI is unable to complete CDD measures in relation to a customer, 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.

VI.130 Where an RFI conducting corporate service provider business decides that a business relationship must be terminated due to an inability to complete CDD, the RFI must take appropriate steps to stop acting as the CSP 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.

VI.131 Where an RFI declines or terminates business due to knowledge, suspicion or reasonable grounds for suspicion that the business might be of criminal intent or origin, the RFI must refrain from referring such a declined business to another person.

Customer transactions or relationships involving cash or bearer instruments

VI.132 In the context of CSP business, RFIs should limit the acceptance or delivery of cash or other bearer negotiable stores of value to de minimus amounts. In extremely rare circumstances where this guidance is not followed, an RFI should be prepared to demonstrate that it has determined and applied appropriate risk-mitigation measures and documented relevant policies, procedures and controls applicable to its business and the particular customer. Any cash or bearer instrument transaction that is not of a de minimus amount should be reported to the RFI's reporting officer.

VI.133 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.

VI.134 Paragraphs 4.99 through 4.103 provide additional guidance on the use of bearer instruments.

Applicability of simplified due diligence to CSP business

VI.135 Simplified due diligence involves the application of reduced or simplified CDD measures in specified circumstances.

VI.136 RFIs may consider applying reduced or simplified due diligence measures only in conformance with the acts, regulations and paragraphs 5.1 through 5.13 and where:

a) The RFI has taken into account the results of Bermuda's national risk assessment;
b) The RFI has conducted and documented a risk assessment providing the RFI with reasonable grounds for believing that there is a low risk of ML/TF; and
c) The RFI has no knowledge, suspicion or reasonable grounds for suspicion of ML/TF.

VI.137 Where a corporate customer's securities are listed on an appointed stock exchange, the corporate is publicly traded and RFIs may forego verifying the identity of the corporate's beneficial owners, provided that:

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

company.

VI.138 Where a corporate is listed outside of Bermuda on a market that is not subject to disclosure obligations equivalent to those in Bermuda, RFIs must apply the verification requirements normally applicable to private and unlisted companies.

VI.139 Where a customer involves an entity for which simplified due diligence is appropriate, RFIs must nonetheless adhere to the guidance notes in identifying and verifying signatories and other persons connected with the customer and its business relationship with the RFI.

VI.140 Detailed information on the applicability of simplified due diligence is set forth in paragraphs 3.18 and 5.1 through 5.13.

Enhanced due diligence for CSPs

VI.141 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.

VI.142 Regulation 11 requires RFIs to apply enhanced due diligence in all situations where a customer or business relationship, or any country or geographic area, service, delivery channel, product or transaction with which the customer engages or the business relationship is involved, presents a higher than standard risk of ML/TF.

VI.143 In addition, enhanced due diligence must be applied in each of the following circumstances:

a) 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 CFATF (see paragraphs 5.17 through 5.19);
b) The customer or beneficial owner has not been physically present for identification purposes (see paragraphs 5.25 through 5.29); and
c) The business relationship or occasional transaction involves a PEP (see paragraphs 5.96 through 5.116).

VI.144 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.

VI.145 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 the persons that comprise, own and control the customer, volume of assets, and information available through public databases;
b) Additional information on the nature of the customer's business and the nature and purpose of the business relationship (see paragraphs 4.1 through 4.4);
c) Additional information on the source of wealth and source of funds of the customer (see paragraphs 5.110 through 5.113);
d) Additional information on the reasons for planned or completed transactions; and
e) Approval of the RFI's senior management to commence or continue the business relationship (see paragraph 5.109).

VI.146 In addition, RFIs should consider applying additional measures, such as:

a) Updating more frequently the identification and verification data for the customer, its beneficial owner(s), and any other persons who own or may exercise control over the customer or who may instruct the RFI on behalf of the customer;
b) Conducting enhanced monitoring of the business relationship by increasing the number and frequency of controls applied and by identifying patterns of activity requiring further examination;
c) Requiring the first payment to be carried out through an account in the customer's name via an RFI subject to the regulations or via an institution that is situated in a country or territory other than Bermuda that imposes requirements equivalent to those in Bermuda, that effectively implements those requirements and that is supervised for effective compliance with those requirements; and
d) Lowering the threshold of ownership below 10% and understanding the voting rights of equity shares to ensure a complete understanding of the control structure of the entity involved.

VI.147 Detailed information on enhanced due diligence is set forth in **Chapter 5: Non-Standard Customer Due Diligence Measures**.

VI.148 Specific indicators of higher risk in CSP business are discussed in greater detail in paragraphs VI.204 through VI.210.

***International Sanctions***

VI.149 RFIs conducting CSP business should implement a sanctions compliance programme in line with the guidance set forth in **Chapter 6: International Sanctions**.

VI.150 RFIs should have in place processes for screening against sanctions, list both customers, prospective customers and any third-party intermediaries seeking to introduce new business, and for performing background checks to identify information about a customer's association with financial or other crime or with

PEPs.

VI.151 RFIs should determine whether any persons connected with a customer and the natural persons connected with any such persons that are legal entities, trusts or other legal arrangements are sanctions targets.

VI.152 RFIs must be aware that, in contrast to AML/ATF measures, which permit CSPs some flexibility in setting their own timetables for verifying (see Regulation 8) and updating CDD information (see 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***

VI.153 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.

VI.154 Ongoing monitoring in the context of corporate service business supports several objectives:

a) Maintaining a proper understanding of a 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 a customer.

VI.155 RFIs conducting CSP business should have adequate policies and procedures in place to confirm that they know on an ongoing basis the current identity of each director, partner or officer and the current identity of all the persons who own and control the entities under administration, including signatories.

VI.156 Failure to adequately monitor a customer's business relationship could expose an RFI to abuse by criminals and may 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.

VI.157 Ongoing monitoring of a 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 customer's conduct are consistent with the RFI's knowledge of the customer, the customer profile, and the persons who own, control and act on behalf of the 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 a customer or person connected with a customer is a PEP and whether a 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 CSP business; and
h) Adjusting risk profiles and risk assessments based on information reviewed.

VI.158 Under the Limited Partnership Act 1883, the Exempted Partnerships Act 1992 and the Limited Liability Company Act 2016, a CSP that maintains a register of members of a limited liability company, or a register of partners of a limited or exempted partnership, unless it holds an unlimited licence, may not register an issue or transfer of securities unless the relevant Bermudian authority has approved. Any such issuance or transfer will be effective only upon notice to the appropriate authority as soon as practicable, but no later than 14 days after the change.

VI.159 RFIs conducting CSP business must ensure that information on the beneficial owners and/or controllers or senior managers of customer companies, partnerships and other legal entities is known to the RFI, properly recorded, up to date, and promptly available for inspection by the BMA and other competent authorities.

VI.160 RFIs conducting CSP business should have detailed policies, procedures and controls in place to make initial determinations of and monitor subsequent changes to beneficial owner and controller information and ensure that their customers file required information with the relevant Bermudian authority.

VI.161 Each RFI should ensure that its policies, procedures and controls dealing with the administration of shelf companies, bearer instruments and nominee arrangements are proportionate to the ML/TF risks involved.

VI.162 An RFI should require corporate customers to notify it of any material change to:

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

VI.163 It is the RFI's responsibility to maintain current information concerning the above.

VI.164 In addition, each time a customer makes a payment of $15,000 or more into a money account, whether the payment is carried out in a single operation or several operations which appear to be linked or otherwise contribute significant value to a business relationship or occasional transaction, an RFI should obtain and verify the source of the funds or value and the objectives of the customer. In such situations, an RFI should determine whether funds received are from known sources on which they have performed CDD or whether the funds are from third parties, foreign accounts or other unknown sources. RFIs should also determine whether the methods of payment and/or the financial instruments used are consistent with the customer's profile, bearing in mind that the use of cash, cashier's cheques, postal money orders, prepaid cards, third-party cheques, cryptocurrencies or other difficult-to-trace payment methods could disguise the origin of the funds.

VI.165 RFIs conducting CSP business should ensure that where a customer transaction would normally be made using a customer account, but the customer requests the transaction to be made using an RFI account, the reasons for this should be understood and evaluated to determine whether the conduct indicates higher ML/TF risk.

VI.166 Ongoing monitoring must be carried out on a risk-sensitive basis. The inherent ML/TF risk levels associated with CSP business should be taken into account when determining baseline levels of ongoing monitoring. Higher-risk customers and business relationships must be subjected to enhanced due diligence and more frequent and/or intensive ongoing monitoring.

VI.167 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 CSP customers and the persons who own and control those customers. See paragraphs 7.11 through 7.14.

VI.168 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.

VI.169 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 in order to understand the nature of the customer's business and the purpose and intended nature of the business relationship with the RFI. See paragraph VI.74.

VI.170 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.

VI.171 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, the persons who own, control and act on behalf of the customer and the business relationship with the RFI. See paragraph VI.59.

VI.172 Detailed information on ongoing monitoring is set forth in **Chapter 7: Ongoing Monitoring**.

***Suspicious Activity Reporting***

VI.173 The suspicious activity reporting requirements for RFIs are governed primarily by Sections 43 through 48 of POCA, Sections 5 through 12 of ATFA, and Regulations 16 and 17.

VI.174 RFIs conducting CSP business 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.

VI.175 The definitions of knowledge, suspicion and reasonable grounds for suspicion are set forth in paragraphs 9.7 through 9.13 of the general GN.

VI.176 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 or not the transaction or conduct is indeed suspicious or provides reasonable grounds for suspicion.

VI.177 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.

VI.178 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.

VI.179 An RFI's reporting officer must consider each report in light of all available information and determine whether it gives rise to knowledge, suspicion or reasonable grounds for suspicion that funds or assets are criminal property or that a person is involved in ML/TF.

VI.180 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.

VI.181 The FIA no longer accepts any manually submitted suspicious activity reports (including those faxed or emailed). It accepts only those suspicious activity reports that are submitted electronically via the goAML system, which is available at **www.fia.bm**.

VI.182 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.

VI.183 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

VI.184 Where an employee fails to comply with the obligations under Section 46 of POCA or Schedule 1 of ATFA to make disclosures to a reporting officer and/or to the FIA promptly after information giving rise to knowledge, suspicion or reasonable grounds for suspicion comes to the attention of the employee; the employee is liable to criminal prosecution.

VI.185 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.

VI.186 Sections 20A through 20I of the 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 power 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.

VI.187 Section 20H of the 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.

VI.188 Section 47 of POCA and Section 10A of ATFA contain tipping-off offences.

VI.189 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 to 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 disclosure.

VI.190 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 personal information or any other matter likely to prejudice the actual or proposed investigation.

VI.191 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.

VI.192 Detailed information on suspicious activity reporting, including related offences and constructive trusts, is set forth in **Chapter 9: Suspicious Activity Reporting**.

***Employee Training and Awareness***

VI.193 The responsibilities of RFIs to ensure appropriate employee training and awareness are governed primarily by Regulations 16 and 18.

VI.194 RFIs must take appropriate measures to ensure that relevant employees:

a) Are aware of the acts and regulations relating to ML/TF;
b) Undergo periodic training on how to identify transactions or conduct which 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.

VI.195 Each RFI must also ensure that relevant employees receive appropriate training on its AML/ATF policies and procedures relating to:

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

VI.196 In a CSP business context, training should enable relevant employees to:

a) Readily identify corporates, partnerships, trusts and other vehicles that may be structured for ML/TF purposes;
b) Understand how beneficial owners are defined under the acts and regulations and be capable of identifying those persons and verifying their identity;
c) Be capable of identifying and verifying the source of wealth and source of funds information;
d) Effectively vet both customers and the persons who own them, control them and act on their behalf;
e) Identify falsified documents;
f) Assess the risks associated with a customer and its business relationship with the RFI;
g) Conduct ongoing monitoring of the customer and its business relationship with the RFI; and
h) Recognise and report transactions or conduct where there is knowledge, suspicion or reasonable grounds for suspicion of ML/TF.

VI.197 Where an employee exercises discretion for or in relation to a customer, the RFI must ensure that the employee 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.

VI.198 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 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.

VI.199 Detailed information on employee training and awareness is set forth in **Chapter 10: Employee Training and Awareness**.

**Record-Keeping**

VI.200 The record-keeping obligations of RFIs are governed primarily by Regulations 15 and 16. As noted in VI.145, RFIs conducting CSP business must ensure that information on the beneficial owners and/or controllers or senior managers of customer companies, partnerships and other legal entities is known to the RFI, properly recorded, up to date and promptly available for inspection by the BMA and other competent authorities.

VI. 201 Under 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.

VI.202 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.

VI.203 Detailed information on the records that must be kept is set forth in **Chapter 11: Record-Keeping**.

***Risk Factors for Corporate Service Provider Business***

VI.204 In addition to the non-exhaustive list of risk factors set forth in paragraph 2.37, RFIs conducting CSP business should consider sector-specific risk factors, including those in paragraphs VI.204 through VI.210 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.

VI.205 Customer and business relationship risk factors include, but are not limited to:

a) The use of 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;
b) A customer establishing a complex legal entity or legal arrangement structure who terminates the business relationship with the RFI soon after the

establishment of the structure where an ongoing relationship would normally be expected;

c) Any unexplained relationship between a customer, the persons acting on behalf of the customer, the persons owning and controlling the customer and any third parties;
d) Management of a customer appears to be acting according to instructions from an unknown or inappropriate person;
e) A person is appointed to a number of unconnected trusts, companies or other legal entities or arrangements, and no nominee arrangement has been disclosed to the RFI;
f) Unjustified delays in the production of identity documents, underlying company accounts or other requested information;
g) The customer or prospective customer appears unwilling or refuses to divulge relevant ownership information or to grant required permissions to third parties to divulge such information for corroboration or verification purposes;
h) The RFI is unable to verify the information a customer provides and/or has reasonable grounds to suspect that the information provided is incorrect, incomplete or otherwise inadequate;
i) A customer who appears to actively and inexplicably avoid face-to-face meetings or who is otherwise evasive, unusually difficult to contact or slow to respond;
j) Situations in which it is difficult to identify the natural persons who own and control a customer, including situations where identification is hindered or delayed because the persons who appear to own or control a customer are legal persons, trusts or other types of legal arrangements;
k) Frequent changes to shareholders, directors or other persons owning or controlling any underlying legal person, trust or other legal arrangement;
l) The unnecessary or excessive use of nominee shareholders or directors;
m) The unnecessary granting of a power of attorney;
n) The use of opaque or complex legal persons or arrangements where the customer is not open about their purpose;
o) The involvement of any PEP as a person owning, controlling or representing the customer, or as a person otherwise connected with the customer;
p) The involvement of any third party or intermediary that would be subject to regulation in Bermuda but that is not subject to equivalent regulation in its jurisdiction;
q) A customer who is unwilling or unable to provide satisfactory information regarding the nature of the customer's business;
r) A customer involved in an industry or sector where opportunities for ML/TF are particularly prevalent;
s) A customer whose activities differ from the RFI's understanding of the nature of the customer's business;
t) Indicators that a customer does not wish to obtain necessary governmental approvals or make required governmental filings;
u) A customer who is unwilling or unable to provide satisfactory information to verify the source of wealth or source of funds;
v) The receipt of funds or assets from un-associated or unknown third parties

where such receipt is not typical;

w) A customer who insists, without adequate justification or explanation, that transactions be effected exclusively or mainly through the use of digital assets for the purpose of obscuring the source of funds or source of wealth and/or to preserve anonymity;
x) Sudden activity from a previously dormant customer without a clear explanation;
y) Levels of assets or transactions that exceed what a reasonable person would expect of a customer with a similar profile;
z) A customer with a previous conviction for a crime that generated criminal property;
aa) A customer offering to pay extraordinary fees for unusual services or for services that would not ordinarily warrant such a premium;
bb) A customer requesting a service or transaction in an unusually tight or accelerated timeframe which would make it difficult or impossible for an RFI to meet its AML/ATF obligations under the acts and regulations; and
cc) A customer who changes the source or means of payment or assets, or the recipient of funds or other assets, at the last minute and without justification.

VI.206 Country and geographic area risk factors include, but are not limited to:

a) A customer entity established with funds originating from foreign banks in high-risk jurisdictions;
b) A customer, person acting on behalf of the customer, person owning or controlling the customer or any third party associated with the customer who is a resident in, or citizen of, a high-risk jurisdiction;
c) A corporate service transaction to or from a high-risk jurisdiction;
d) A non-face-to-face corporate service transaction initiated from a high-risk jurisdiction;
e) A corporate service transaction linked to business in or through a high-risk jurisdiction;
f) CSP business involving persons or transactions with a material connection to a jurisdiction, entity, person, good, service or activity that is a target of an applicable international sanction;
g) Requests for the use of a pre-constituted shell company in a jurisdiction that allows the company's use but does not require ownership and control information to be updated; and
h) A corporate service business relationship or transaction for which an RFI's ability to conduct full CDD may be impeded by a jurisdiction's confidentiality, secrecy, privacy or data protection restrictions.

VI.207 Products and services risk factors include, but are not limited to:

a) The unexplained and illogical use of corporate structures, legal arrangements, shelf companies, split boards, nominee shares or bearer negotiable instruments;
b) Any request for advice on establishing a legal entity or legal arrangement

structure for the purpose of, or with the effect of, making it more difficult for competent authorities to determine the structure's beneficial owners or beneficiaries;

c) Any request for an RFI to represent or assure a customer's standing, reputation or credibility to third parties, where the RFI is unable to develop a commensurate understanding of the customer's affairs;
d) The unexplained and illogical use of mail hold or care of (c/o) mail services;
e) Any request that might indicate that the stated purpose of the customer's structure, the stated nature of the customer's business or the stated purpose of the customer's business relationship with the RFI is not the true purpose or nature;
f) Any request to manage a customer's finances or bank accounts where such a customer would ordinarily manage its own finances and banking;
g) 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;
h) Requests for use of a pre-constituted shell company in a jurisdiction that allows the company's use but does not require ownership and control information to be updated;
i) Requests to create a corporate structure or carry out a transaction with undue complexity or with no discernible commercial purpose;
j) Requests to create a corporate structure or to carry out a transaction with undue speed, particularly where the person associated with the customer requests that any of the due diligence processes be completed after the establishment of the entity or after the initiation of a transaction; and
k) Requests for anonymity. While a customer's requests for their business to be conducted discreetly should not automatically be inferred as illegitimate, anonymity requests may indicate higher risk.

VI.208 Transaction risk factors include, but are not limited to:

a) A customer that, once established, receives sizeable or multiple cash deposits or deposits from multiple sources;
b) Successive capital or other contributions in a short period of time to the same company with no apparent legal, tax, business, economic or other legitimate purpose;
c) Transactions involving gambling, money service businesses or cash-intensive businesses, or the proceeds of such categories of business;
d) Transactions involving prohibited items such as armaments;
e) Large cash transactions in circumstances where such a transaction would normally be made by cheque, banker's draft or wire transfer;
f) Transfers of funds without a clear connection to the actual activities of the customer entity;
g) Transfers of funds that are not in line with the stated nature of the customer's business;
h) A payment to or from a third party without any justifiable rationale;
i) Customers requesting transfers to or from overseas locations with instructions for payment to be made in cash;

j) Sizeable third-party cheques endorsed in favour of the customer or a person associated with the customer;
k) Large payments for unspecified services to consultants, employees or other parties;
l) Purchase or sale transactions significantly above or below the market price, involving multiple invoicing of the same goods or services, or involving falsely described or falsely quantified goods or services;
m) Commercial, private or real property transactions that have no apparent legitimate business, tax, legal or family governance purpose;
n) Transactions for which the customer provides inconsistent or irrational explanations and which the customer is subsequently unwilling or unable to explain by reference to legal, tax, business, economic or other legitimate purposes;
o) Attempts by a customer to enter into a fraudulent transaction or to enter into any arrangement to fraudulently evade tax;
p) Known prior associations between the parties to a transaction or other indications that a transaction is not being conducted on an 'arm's length' basis;
q) Unusual, complex or uncharacteristically large transactions;
r) Transactions of a size or volume that exceed what a reasonable person would expect of a customer with a similar profile, or given the nature and stated purpose of the business relationship or transaction;
s) Occasional transactions giving rise to suspicion; and
t) 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.

VI.209 Delivery channel risk factors include, but are not limited to:

a) Non-face-to-face relationships with customers and the 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 or source of funds of any of the parties to the transaction; and
c) The use of a third-party intermediary, agent or broker, particularly where such a person would be subject to regulation in Bermuda but is not subject to equivalent regulation in its jurisdiction.

VI.210 Third-party risk factors include, but are not limited to:

a) The involvement of any third party in carrying out any AML/ATF function in relation to a customer, including the reliance upon or outsourcing to any 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). This includes any involvement of a 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;
iii. Impede the effective ability of the appropriate regulator to monitor the RFI's compliance with all obligations under the regulatory system;
iv. Reduce the responsibility of the RFI and/or its managers and officers;
v. Remove or modify any conditions subject to which the RFI's authorisation was granted; or
vi. Increase ML/TF risk in any way that is not adequately addressed through appropriate risk assessment and mitigation;

b) Any unexplained relationship between a customer, the persons acting on behalf of the customer, the persons owning and controlling the customer and any third parties; and
c) The use of a third-party intermediary, agent or broker, particularly where such a person would be subject to regulation in Bermuda but is not subject to equivalent regulation in its jurisdiction.

***