Annex VIII

Sector-Specific Guidance Notes (SSGN) for Digital Asset Business

These SSGN are annexed to, and should be read in conjunction with, the general Guidance Notes for Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) Regulated Financial Institutions on AML/ATF 2021 (GN)

ANNEX VIII

SSGN FOR DIGITAL ASSET BUSINESS

Introduction

VIII.1 This annex sets forth guidance on AML/ATF obligations under the acts and regulations of Bermuda that are specific to Digital Asset Business (DAB).

VIII.2 Under Section 42A(1)(i) of POCA, a person that is a licensed undertaking carrying on DAB within the meaning of Section 4 of the Digital Asset Business Act 2018 (DABA) is designated as an AML/ATF regulated financial institution (RFI).

VIII.3 Under Section 4 of DABA, a person carries on DAB in Bermuda if the person is:

a) incorporated or formed in Bermuda and carries on any digital asset activity set out under Section 2(2) of DABA;
b) incorporated or formed outside of Bermuda and carries on any DAB activity set out under Section 2(2) of DABA in or from within Bermuda; or
c) otherwise regarded as carrying on DAB in or from Bermuda in accordance with an order made by the Minister of Finance.

VIII.4 Under Section 2(2) of DABA, DAB means the business of providing any or all the following DAB activities to the public:

1. <u>Issuing, selling or redeeming virtual coins, tokens or any other form of digital asset</u>

   Persons within this category include, for example, those who assist others in designing a coin or token or in administering an initial coin offering (ICO) or token. This category generally does not include a person that solely issues a coin or token to fund the person's own operations.

2. <u>Operating as a payment service provider business utilising digital assets, which includes the provision of services for the transfer of funds</u>

   Part 4, Section 21 of the POCR defines a payment service provider as "a person whose business includes the provision of services for the transfer of funds." For purposes of these SSGN, digital assets are funds. See paragraph VIII.11.

3. <u>Operating as a digital asset exchange</u>

   Under Section 2(1) of DABA, a digital asset exchange is a marketplace used for digital asset issuances, distributions, conversions and trades, including

primary and secondary distributions, with or without payment, provided that digital asset conversions and trades may also be entered into by the electronic marketplace as principal or agent. A digital asset exchange may enable customers to buy, sell and trade digital assets. A purchase, sale or trade using a digital asset exchange may involve the exchange of one digital asset (e.g., a coin or token) for another digital asset, or the exchange of a digital asset for fiat currency (e.g., dollars).

4. Carrying on digital asset trust services

Under Section 2(1) of DABA, a person carries on digital asset trust services if the person carries on the business of acting as a fiduciary, agent or trustee on behalf of another person for the purpose of administration and management of a digital asset.

5. Providing custodial wallet services

Under Section 2(1) of DABA, a wallet is a software program that stores private and public keys and interacts with distributed ledger technology to enable users to send, receive and monitor their digital assets. A person provides custodial wallet services if the person provides the services of storing or maintaining digital assets or a virtual wallet on behalf of a client. A person, generally, is not a custodial wallet service provider solely by virtue of developing wallet software.

6. Operating as a digital asset derivative exchange provider

Under Section 2(1) of DABA, a digital asset derivative is an option, swap, future, contract for difference or any other contract or instrument whose market price, value or delivery or payment obligations are derived from, referenced to or based on a digital asset underlying interest. A digital asset derivative exchange is a centralised or decentralised marketplace used for digital asset derivatives issuances, distributions and trades with or without payment, provided that digital asset derivatives trades may also be entered into by the marketplace as principal or agent. A digital asset derivative exchange provider is a person operating a digital asset derivative exchange and that provides the services of creating, selling or otherwise entering into digital asset derivatives contracts, or that provides the services of clearing and settlement of digital asset derivatives.

7. Operating as a digital asset services vendor

Under Section 2(1) of DABA, a digital asset services vendor includes a person that:

a) under an agreement as part of its business—
   i. can undertake a digital asset transaction on behalf of another person;

ii. has power of attorney over another person's digital asset;

b) operates as a market maker for digital assets; or
c) operates as a digital asset benchmark administrator.

VIII.5 A person who carries out digital asset transactions solely for their own account, and who does not provide any DAB activities to the public, is not carrying on DAB as defined under Section 2(2) of DABA. To the extent that such a person is not otherwise brought within the definition of an RFI under Section 42A(1) of POCA, such a person is not an RFI.

VIII.6 Under Section 10 of DABA, a person that carries on DAB in or from Bermuda must be a licensed undertaking, unless exempted by or under an order issued by the Minister of Finance.

VIII.7 Under Section 10 of DABA, persons conducting DAB must obtain a licence from the BMA prior to commencing business in Bermuda. Persons who would be obligated to obtain a licence under Section 10 may be exempted from the licensing requirement by an exemption order pursuant to Section 11. Such persons are nonetheless RFIs.

VIII.8 All RFIs must comply with the acts and regulations, and with the main AML/ATF GN issued by the BMA.

VIII.9 Schedule 1, Section 2(3) of DABA states that in determining whether a licensed undertaking is conducting its business in a prudent manner, the BMA will take into account any failure to comply, among other things, with:

a) POCA;
b) The Anti-Terrorism (Financial and Other Measures) Act 2004;
c) POCR;
d) DABA;
e) Relevant codes of practice issued by the BMA, including, for example, the Digital Asset Business (Prudential Standards) (Annual Return) Rules 2018; and
f) International sanctions in effect in Bermuda.

VIII.10 For the purposes of this SSGN, the terms "AML/ATF regulated financial institution" and "RFI" should be understood to include licensed undertakings carrying on DAB within the meaning of Section 4 of DABA, and persons who would be obligated to obtain a licence under Section 10 of DABA, but who have been exempted from the licensing requirement by an exemption order pursuant to Section 11. The term "digital asset business" should be understood to include all the activities described in paragraph VIII.4.

VIII.11 The BMA considers references to the terms "funds" and "securities" in POCA, ATFA, POCA SEA, POCR, the general GN, and Annexes to the GN to include digital assets that share similar qualities to "funds" or "securities." For

example, an RFI conducting DAB that involves the transfer of a digital asset is likely a payment service provider or digital asset exchange.

VIII.12 In addition, the BMA understands references to dollar amounts in POCA, ATFA, POCA SEA, POCR, the general GN, and Annexes to the GN to be references to digital assets with an equivalent value in dollars. For the purposes of determining whether a digital asset transaction meets a regulatory threshold, for example, for determining whether a transaction is an occasional transaction, RFIs should consider the equivalent value, in dollars, of the digital asset transaction.

VIII.13 RFIs conducting DAB should read these SSGN in conjunction with the general GN. This annex supplements, but does not replace, the general GN.

VIII.14 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.

VIII.15 Portions of this annex include sector-specific information, such as risk indicators that are particular to DAB. This sector-specific information should be considered as supplementary to the general GN.

Status of the guidance

VIII.16 Pursuant to Section 49M of POCA and 120 of ATFA, these SSGN 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's website at www.bma.bm.

VIII.17 These SSGN are of direct relevance to all senior management, inclusive of the compliance officer, and to 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).

VIII.18 The Court, or the BMA, as the case may be, in determining whether a person is in breach of a relevant provision of the acts or regulations, is required to consider whether a person has followed any relevant guidance approved by the Minister of Legal Affairs and 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 of, and paragraph 1(6) of Part I, Schedule I to ATFA and Section 20(6) of POCA SEA.

VIII.19 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.

VIII.20 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.

VIII.21 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.

VIII.22 RFIs should be aware that under Section 16(1) of the Financial Intelligence Agency Act 2007, the FIA may, in the course of enquiring into a suspicious transaction or activity relating to ML/TF, serve a notice in writing on any person requiring the person to provide the FIA with such information as it may reasonably require for the purpose of its enquiry.

VIII.23 Detailed information is set forth in the general GN beginning with the **Preface**.

Senior management responsibilities and internal controls

VIII.24 The AML/ATF responsibilities for senior management of an RFI conducting DAB are governed primarily by POCA, POCA SEA, ATFA and POCR Regulations 16 through 19.

VIII.25 The AML/ATF internal control requirements for RFIs conducting DAB are governed primarily by Part 3 of the POCR Regulations.

VIII.26 POCR Regulation 19 provides that failure to comply with the requirements of specified POCR 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.

VIII.27 Section 20 of POCA SEA empowers the BMA to impose a civil penalty on any person supervised by the BMA in an amount up to $10,000,000 for each failure to comply with specified POCR Regulations. POCA SEA also provides for several criminal offences, including carrying on business without being registered pursuant to Section 9 of DABA.

VIII.28 Senior management of DAB 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.

VIII.29 Under Bermuda's acts and regulations, 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.

VIII.30 RFIs must establish and maintain detailed policies, procedures and controls that are adequate and appropriate to forestall and prevent operations related to ML/TF.

VIII.31 RFIs should consider using proven technology-driven solutions to minimise the risk of error and find efficiencies in their AML/ATF processes.

VIII.32 Under Section 12(6)(c) of DABA, an RFI conducting digital asset business must include its AML/ATF policies and procedures with its application to become a licensed undertaking under DABA. In addition, the Information Bulletin regarding the Assessment and Licensing Committee (ALC) Digital Asset Business Application Process (BMA – September 2018) requires each RFI conducting DAB to include an overview of its risk appetites with its application. RFIs should also submit a business risk assessment and client risk assessment at the time of application.

VIII.33 Under Schedule 1, paragraph 5 (Consolidated supervision) of DABA, an RFI conducting digital asset business must ensure that the position of the RFI within the structure of any group to which it may belong will not obstruct the conduct of effective consolidated supervision.

VIII.34 The Digital Asset Business (Prudential Standards) (Annual Return) Rules 2018 require each licensed DAB to submit an annual return that confirms, among other information:

a) Whether senior management approval is required to approve new business,

if the client has been risk-rated as low, medium or high;

b) If senior management approval is required to retain an existing client, if the client's risk rating has changed to low, medium or high;
c) Whether the powers, roles, responsibilities and accountabilities between it, its board of directors (board) and senior management are clearly defined, segregated and understood by all;
d) Whether the board and senior management understand how it operates through structures that may impede transparency;
e) That the board, or any related board committee, assists senior management in fulfilling its oversight function through the review and evaluation of the financial reporting process and adequacy and effectiveness of the system of internal controls, including financial reporting and information technology security controls;
f) Confirmation that the board receives sufficient AML/ATF information to assess and understand the senior management's process for evaluating its system of internal controls;
g) Whether the board ensures that it complies with all relevant laws and regulations and endeavours to adopt best AML/ATF practices;
h) That the board and senior management declare any conflicts dealings to the compliance department (or other relevant internal body) when applicable or required;
i) That senior management provides oversight to the licensed undertaking with regard to enterprise risk management and identifies key risk areas and key performance indicators and monitors these factors with due diligence;
j) Whether the board ensures there is appropriate oversight by senior management that is consistent with its policies and procedures;
k) Whether senior management sets and enforces clear lines of responsibility and accountability throughout the organisation;
l) That, at least annually, the board monitors the senior management's compliance with any strategy and direction policies set by the board and senior management's performance based on approved targets and objectives;
m) That the board receives advice on all major financing transactions, principal agreements and capitalisation requiring board approval and senior management makes appropriate recommendations for the board's consideration;
n) Whether the compliance and audit function are independent of all operational and business functions, when practicable; and whether such functions have direct lines of communication to the board; and
o) That it has instituted policies or procedures to provide for the senior compliance officer to have regular contact with and direct access to the board to ensure that the board is able to satisfy itself that its statutory obligations are being met and the measures taken to prevent risks of ML/TF are sufficiently robust.

VIII.35 Where a Bermuda RFI conducting DAB 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.

VIII.36 Attempts to launder money through DAB 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 DAB; and
c) Indirectly, by a third-party service provider or by an RFI, independent professional or other intermediary facilitating transactions involving illicit assets on behalf of another person.

VIII.37 Most of this annex addresses attempted ML by customers. ML risks involving third parties are addressed primarily in paragraphs VIII.126 through VIII.132. ML risks involving internal senior management, directors, managers or employees are addressed primarily via the fit and proper requirements for DABs and in paragraphs VIII.43 through VIII.47.

VIII.38 Specific requirements for an RFI's detailed policies, procedures and controls are set forth in **Chapters 2 through 11** of the general GN.

VIII.39 Detailed information is set forth in **Chapter 1: Senior Management Responsibilities and Internal Controls**.

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

VIII.40 Persons carrying on DAB 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) DABA;
b) The Digital Asset Business (Prudential Standards) (Annual Return) Rules 2018; and
c) Digital Asset Issuance Rules 2020.

VIII.41 Persons carrying on DAB may also be subject to the requirements, principles, standards and procedures set forth in guidance documents. These guidance documents for DAB include, but are not limited to:

a) Statement of Principles (BMA – September 2018) made pursuant to Section 5 of DABA;
b) Code of Practice (BMA – September 2018) made pursuant to Section 6 of DABA;
c) Information Bulletin: Assessment and Licensing Committee (ALC) Digital

Asset Business Application Process (BMA – September 2018);

d) Statement of Principles (BMA – June 2020) made pursuant to Section 7 of the Digital Asset Issuance Act 2020; and
e) Digital Asset Custody Code of Practice (BMA – May 2019) made pursuant to Section 6 of DABA.

VIII.42 The requirements of the acts, regulations and additional guidance documents described in paragraphs VIII.40 through VIII.41 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 guidance notes, whether as part of its existing business processes or through separate processes.

Ownership, management and employee checks

VIII.43 To guard against potential ML involving owners, directors, managers and employees of DABs, POCR Regulation 18(1)(c) requires RFIs conducting DAB to screen such persons against high standards. Additional guidance on screening and probity is set forth in paragraphs 1.73 through 1.77 of the general GN, and the Digital Asset Custody Code of Practice (BMA – May 2019) and Statement of Principles (BMA – September 2018) described in paragraph VIII.41.

VIII.44 The Digital Asset Business (Prudential Standards) (Annual Return) Rules 2018 require each licensed DAB to submit an annual return that confirms, among other information:

a) Whether it has established and is, on an ongoing basis, maintaining and operating appropriate procedures in order to be satisfied of the integrity of new employees;
b) Whether the incidence of financial crime committed by employees (e.g., theft, fraud) is low;
c) That employees are required to declare personal dealings relevant in the jurisdictions that it operates in on a regular basis (at least annually); and
d) That the following actions are undertaken when recruiting staff:
    i. Verify name;
    ii. Verify residential address;
    iii. Check if the individual should be considered a PEP (see paragraphs 5.96 through 5.115 of the general GN);
    iv. Check individual against sanctions lists;
    v. Check for any negative press against the individual;
    vi. Confirm employment history;
    vii. Confirm references;
    viii. Request details on any regulatory action taken against the individual; and

ix. Request details of any criminal convictions.

VIII.45 RFIs should ensure that screenings are conducted both for the RFI itself and for any agent, intermediary or third-party service provider.

VIII.46 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.

VIII.47 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 DAB will need to undertake to meet its screening obligations.

Monitoring and Managing Compliance

VIII.48 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 POCR Regulations are in place; and
b) Coordinate and monitor the compliance programme to ensure continuous compliance with the POCR Regulations.

VIII.49 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.

VIII.50 The role, standing and competence of the compliance officer and the reporting officer, and the manner in which the RFI's policies, procedures and controls are designed and implemented, impact directly on the effectiveness of an RFI's AML/ATF arrangements, and the degree to which the RFI 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.

VIII.51 The Digital Asset Business (Prudential Standards) (Annual Return) Rules 2018 require each licensed DAB to submit an annual return that confirms, among

other information:

a) Its compliance officer's work arrangement;
b) Its reporting officer's work arrangement;
c) Whether the compliance officer is located in Bermuda;
d) Whether the reporting officer is located in Bermuda; and
e) Whether the compliance officer is a member of senior management.

Risk-based approach for RFIs conducting DAB

VIII.52 As described in **Chapter 2: Risk-Based Approach**, RFIs, including those conducting DAB, 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, each DAB 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 higher-risk;
d) The jurisdictions the DAB 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 the FATF or the CFATF; and
e) The internal audit function and regulatory findings.

VIII.53 The NAMLC has publicly released a report on Bermuda's national assessment of ML/TF risks. RFIs should consider the results available to them from this and future national risk assessments.

VIII.54 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.

VIII.55 When designing and evaluating a new product or service, an RFI conducting DAB must, prior to launch, assess the risk of the product or service being used for ML/TF.

VIII.56 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.

VIII.57 RFIs conducting DAB 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.

VIII.58 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.

VIII.59 The higher the risk an RFI faces from any 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.

VIII.60 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.

VIII.61 RFIs conducting DAB 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.

VIII.62 Although RFIs conducting DAB 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.

VIII.63 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**.

ML/TF risks in DAB

VIII.64 Using the risk-based approach, each RFI conducting DAB should determine its risk tolerance, which is the amount of ML/TF risk the RFI will accept in pursuit of its business goals.

VIII.65 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.

VIII.66 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.

VIII.67 The Digital Asset Business (Client Disclosure) Rules 2018 require each licensed DAB, prior to entering an initial transaction for, on behalf of or with a client, to disclose to the client all material risks associated with the licensed undertaking's products, services and activities.

VIII.68 The Digital Asset Business (Prudential Standards) (Annual Return) Rules 2018 require each licensed DAB to submit an annual return that contains, among other information:

a) The licensed undertaking's AML/ATF risk self-assessment and risk management policies;
b) Details of products, and product features, including whether any product has an enhanced anonymity feature, and services;
c) Whether clients are risk-rated for ML/TF risk; and
d) The number of clients in each of the following risk assessment categories: "low risk", "medium risk", "high risk" and "unknown".

VIII.69 The Information Bulletin regarding the Assessment and Licensing Committee (ALC) Digital Asset Business Application Process (BMA – September 2018) requires each RFI conducting DAB to include an overview of its risk appetites with its application for a licence.

VIII.70 The DAB sector is often considered as posing a higher risk of ML/TF. Criminals may be attracted to the sector because DAB:

a) Is a newly regulated sector that remains unregulated in many jurisdictions;
b) Products and services may be used to facilitate anonymity or to exploit a false identity;
c) Transactions are often fast, simple and irreversible;
d) Transactions may be cross-border with a global reach;
e) Transactions often involve cash- or other bearer instrument-like digital assets that may be transacted in without the involvement of an RFI;
f) It may involve one-off transactions outside of an established business relationship that could be otherwise more readily monitored for uncharacteristic behaviour; and
g) It may involve agents, exchanges or other intermediaries or service providers that do not follow appropriate AML/ATF policies, procedures

and controls.

VIII.71 Although some digital assets or DABs may be abused by criminals for ML/TF purposes, the level of inherent risk associated with a particular digital asset or DAB depends upon several factors, including, but not limited to:

a) The specific digital asset products and services the business offers;
b) The volume of activity being conducted through the business;
c) The extent to which agents, intermediaries, branches or third-party service providers are involved in the business;
d) The complexity of any payment chains used;
e) The geographic areas in which the business operates; and
f) The identity, activities and geographic origin of the business' customers.

VIII.72 The level of inherent ML/TF risk associated with DAB may be higher where the business:

a) Deals significantly in cross-border transactions;
b) Deals significantly in one-off transactions that are frequent and/or large in terms of equivalent fiat currency;
c) Offers several digital asset products or services;
d) Is located in, or transacts with or through persons or equipment that are from or in a geographic area considered to be high-risk for ML/TF or other criminal activity (see paragraph 5.19 of the general GN); or
e) Can be traced to or from a known or suspected mixer or tumbler service, the dark web or any other higher-risk person.

VIII.73 Mixing services, also called "mixer" or "tumbling" services, are services designed to obscure the origin of a digital asset, or to otherwise facilitate an anonymous transfer of a digital asset from a person or blockchain location to another person or blockchain location. Any association of a client or transaction with a mixing service is an indicator of high ML/TF risk.

VIII.74 The dark web is a part of the World Wide Web that can be accessed only using special software, such as The Onion Router (TOR) network, and is often used with the objective of increasing anonymity for website operators and users. Any association of a client or transaction with the dark web is an indicator of high ML/TF risk.

VIII.75 The level of inherent ML/TF risk associated with DAB may be lower where the business:

i.

a) Primarily markets to customers conducting, what the DAB has determined to be, routine transactions (relative to the customers' nature of business) with moderate frequency in low or expected amounts;
b) Is a digital asset transmitter that only remits virtual funds to confirmed domestic entities, particularly where both the customer and recipients are

RFIs and are subject to AML/ATF regulations;
c) Offers only a single lower-risk DAB product or service; or
d) Processes both sides of a transaction primarily for confirmed local residents.

VIII.76 Where a DAB offers only a single product or service, the RFI's risk assessment should nonetheless identify categories of customers and transactions that are higher or lower-risk within that single product or service. The RFI must also evaluate whether a product, service, transaction or customer has links to privacy or anonymity features or services that increase the level of inherent ML/TF risk and, if so, the RFI must record in its risk assessment the RFI's evaluation and the commensurate risk-mitigation measures it will take.

VIII.77 ML/TF risks associated with DAB should be reduced through the application of mitigation measures that are commensurate to the risks the business identifies.

VIII.78 Examples of measures that may be used to mitigate an RFI's identified ML/TF risks include, but are not limited to:

a) Obtaining and verifying additional customer information (see paragraphs 5.50 through 5.62 of the general GN);
b) Usage limits (see paragraphs 5.63 through 5.70 of the general GN);
c) Geographic limits (see paragraphs 5.71 through 5.75 of the general GN);
d) Increased monitoring and record-keeping, including blockchain analysis and the maintenance of searchable historical transaction information (see paragraphs 5.76 through 5.81 of the general GN); and
e) Due diligence and controls to mitigate the risk of a product and service that relies upon multiple parties for its operation (see paragraphs 5.82 through 5.93 of the general GN).

VIII.79 Additional guidance regarding new payment methods, including DAB, and related mitigation measures is set forth in paragraphs 5.36 through 5.49 of the general GN.

VIII.80 Specific indicators of higher risk in DAB are discussed in detail in paragraphs VIII.241 through VIII.246 of this annex.

CDD

VIII.81 RFIs conducting DAB must carry out CDD.

VIII.82 Detailed information on CDD is set forth in **Chapters 3, 4 and 5** of the general GN, and paragraphs VIII.83 through VIII.178 of this annex.

VIII.83 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 DAB customers or activities being investigated.

VIII.84 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. 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.

VIII.85 An RFI conducting DAB 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 way fees are expected to be deducted or paid; and
c) State how and by whom authorised requests for action are to be given.

VIII.86 Detailed information on CDD for legal persons and other legal arrangements is set forth in paragraphs 4.61 through 4.143 and Annex I.

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

business relationship

VIII.87 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.

VIII.88 An RFI should obtain information sufficient for it to be reasonably satisfied that there is a legal commercial or personal rationale for the DAB work undertaken.

VIII.89 To obtain an understanding sufficient to monitor a DAB relationship or transaction, an RFI should collect information, including, but not limited to:

a) The customer's goals for the DAB relationship or transaction;
b) The source of wealth and source of funds to be used in the DAB relationship or transaction;
c) The anticipated type, volume, value, frequency, duration and nature of the activity that is likely to be undertaken through the DAB 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 DAB relationship or occasional transaction;
e) The means of payment (e.g., cash, wire transfer, other means of payment); and
f) 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

VIII.90 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.

VIII.91 RFIs should make enquiries as to how a customer has acquired the wealth, whether in digital assets, currency, securities or any other assets, to be used in the DAB relationship or transaction.

VIII.92 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.

VIII.93 RFIs should also ensure that they understand the source of funds and specific means of payment, including the details of any account that a customer proposes to use.

VIII.94 Additional information on 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 DAB context

VIII.95 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 DAB relationship or transaction may involve more than one person who is a customer.

VIII.96 The term "business relationship" means a business, professional or commercial relationship between an RFI and a customer, which, at the time contact is first made, the RFI expects to have an element of duration. A business relationship is also formed where the expectation of duration is not initially present but develops over time. A relationship need not involve the RFI in an actual transaction; giving advice may often constitute the establishment of a business relationship.

VIII.97 The term "occasional transaction" for RFIs means a transaction carried out other than as part of a business relationship, amounting to $15,000 or more, whether the transaction is carried out in a single operation or several operations that appear to be linked. The term "occasional transaction" also means any transfer of funds, digital asset payment or wire transfer carried out in an amount of $1,000 or more.

VIII.98 Where a customer who has carried out an occasional transaction, amounting to less than $15,000, requests a future or ongoing service, or returns to carry out further transactions, the RFI should consider that it is entering into a business relationship requiring CDD measures.

VIII.99 Linked transactions may be a series of transactions involving a customer, or they may be transactions that appear to be independent but are, in fact, split into two or more transactions to avoid detection, CDD requirements or questions about the source of wealth or source of funds.

VIII.100 RFIs should have systems to identify and detect linked transactions, to apply enhanced due diligence to them and to 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.

VIII.101 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.

VIII.102 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.

VIII.103 A customer that is not a private, natural person generally involves several 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.

VIII.104 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 a DAB product or service;
b) Each **agent** and each **agent's principal** involved in a business relationship or one-off transaction; and
c) Each **beneficial owner** of a customer.

VIII.105 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.

VIII.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.

VIII.107 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 DAB context

VIII.108 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.

VIII.109 Under POCR Regulation 3, an RFI conducting DAB must consider as beneficial owners any persons, whether natural persons, legal persons or legal arrangements, that effectively own or control more than 25% of a customer's funds, assets or voting rights or, in the case of trusts or similar legal

arrangements, any person who is entitled to a specified interest in the trust property. 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.

VIII.110 Where control or ownership 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.

VIII.111 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.

VIII.112 Information on the identification and verification of beneficial owners is set forth in POCR Regulation 3 and **Chapter 4: Standard Customer Due Diligence Measures**.

VIII.113 Additional information specific to the beneficial ownership of trusts is set forth in POCR Regulation 3(3) and paragraphs I.78 through I.87. Information specific to control over a trust is set forth in POCR Regulation 3(4) and paragraphs I.65 through I.70.

<u>Obtaining and verifying customer identification information</u>

VIII.114 RFIs must obtain and verify identification information for each person who is a customer in the DAB context.

VIII.115 A person who is a customer in the DAB context may be a natural person, legal person, trust or other legal arrangement. For each type of customer, an RFI should follow the identification and verification requirements in **Chapter 4: Standard CDD Measures**, as supplemented by any relevant Annexes.

VIII.116 In addition to the customer identification and verification measures described in **Chapter 4: Standard CDD Measures**, as supplemented by any relevant Annexes, RFIs conducting DAB should also consider identifying and verifying other customer information, including, but not limited to:

a) Blockchain or wallet addresses a customer uses;

b) Public keys associated with a customer;
c) The internet protocol (IP) address(es) a customer uses when interacting with the RFI; and
d) Geolocation data indicating a customer's physical location when interacting with the RFI.

Obtaining and verifying beneficial owner information

VIII.117 RFIs conducting DAB must obtain and verify 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 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 25% 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.

VIII.118 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.

VIII.119 Information on the identification and verification of beneficial owners is set forth in POCR Regulation 3 and **Chapter 4: Standard CDD Measures** of the general GN.

VIII.120 Additional information specific to the beneficial ownership of trusts is set forth in POCR Regulation 3(3) and paragraphs I.78 through I.87 of Annex I.

Timing of CDD

VIII.121 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 that appear to be linked, or carries out any transfer of funds, digital asset payment or 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.

VIII.122 Without exception, RFIs conducting DAB 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.

VIII.123 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.

VIII.124 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.

VIII.125 Detailed information on the timing of CDD measures is set forth in **Chapter 3: Overview of Customer Due Diligence**.

Previous due diligence and reliance on third parties

VIII.126 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.

VIII.127 Where reliance is permissible, the following duties cannot be delegated to a relied-upon person; they remain with the relying RFI:

a) Conducting ongoing monitoring to scrutinise transactions undertaken throughout the course of the relationship to ensure that the transactions are consistent with the RFI's knowledge of the customer, beneficial owners, nature of the customer's business, purpose and intended nature of the business relationship and, where necessary, the source of funds or wealth; and
b) Reporting knowledge of suspicion of ML/TF.

VIII.128 In any reliance situation, the relying RFI retains responsibility for any failure

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

VIII.129 Before an RFI conducting DAB 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.

VIII.130 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 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.

VIII.131 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.

VIII.132 Where, however, an RFI determines that relevant documentation is not available, or is inadequate, the RFI must seek additional documentation.

Outsourcing

VIII.133 An outsourcing arrangement occurs where an RFI conducting DAB uses a service provider to perform an activity, such as applying CDD measures, that would normally be carried out by the RFI. Irrespective of whether the service provider is in Bermuda or overseas, and irrespective of whether the service provider is within or independent of any financial group of which the RFI may be a member, any outsourcing arrangement is subject to the POCR Regulations, including Regulation 14, and both these SSGN and the general GN.

VIII.134 Outsourced activities must be carried out in accordance with the RFI's policies, procedures and controls. The RFI must have specific policies, procedures and controls for monitoring and managing any service provider to which the RFI outsources an activity relating to AML/ATF. In addition, the RFI must ensure that the service provider has in place AML/ATF systems, controls and procedures that comply with Bermuda AML/ATF requirements. An RFI's board or similarly empowered body or natural person, such as the compliance officer, must clearly define and document the roles, responsibilities and duties or persons responsible for all outsourced activities, as if the activities were performed in-house according to the RFI's own standards of internal control and oversight.

VIII.135 In any outsourcing arrangement, an RFI conducting DAB cannot contract out its statutory and regulatory responsibilities to prevent and detect ML/TF.

VIII.136 The Digital Asset Business (Prudential Standards) (Annual Return) Rules 2018 require each licensed DAB to submit an annual return that contains, among other information:

a) The names of outsourcing partners; and
b) Copies of service level agreements setting out the roles, duties and functions of outsourced partners; including third parties or affiliates of outsourced partners performing compliance and other key functions of the licensed undertaking.

VIII.137 Detailed information on outsourcing is set forth in paragraphs 5.149 through 5.174 of the general GN.

Agent networks and other third parties

VIII.138 Where an RFI's DAB involves an agent network, or other third parties, the RFI should ensure that the agent or other third party has in place appropriate policies, procedures and controls to assess and mitigate the ML/TF risks associated with their involvement in the DAB.

VIII.139 RFIs should require agents and other third parties to demonstrate that they are effectively supervised for compliance with appropriate AML/ATF obligations.

VIII.140 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, be 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 the purposes of AML/ATF. Still, other agents may be most accurately considered as customers entering 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.

VIII.141 RFIs that provide services with the involvement of other parties must determine the distribution of AML/ATF responsibilities between the parties.

VIII.142 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 onboarding 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 VIII.147, 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 SSGN and the general GN.

After onboarding the agent:

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 is merited;
e) Take prompt corrective action as needed, including filing SARs about the agent, where appropriate; and
f) Terminate the relationship where appropriate.

VIII.143 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.

VIII.144 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.

VIII.145 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 POCR Regulations, as this responsibility cannot be delegated.

VIII.146 RFIs conducting DAB 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 for compliance with, an appropriate AML/ATF regulatory regime.

VIII.147 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 twelve 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 DAB on behalf of the RFI; and
h) The number, if any, of branches or sub-agents the agent has.

Money transmission and wire transfers

VIII.148 Any RFI, including an RFI conducting DAB, that provides services for the transfer of digital assets, money transmission, or other transfer of funds, is a payment service provider (PSP) engaging in a wire transfer and is 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.

VIII.149 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.

VIII.150 Complete information on the payer means:

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

VIII.151 Complete information on the payee means:

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

VIII.152 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.

VIII.153 Where a payer or payee does not have an account number, the PSP must

substitute it with a unique identifier that allows the transaction to be traced to the payee. See paragraph 8.33 of the general GN.

VIII.154 RFIs conducting DAB 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 RFI conducting DAB should ensure that its terms and conditions of business with each payer address the release of the complete information described in paragraphs 8.9 through 8.19 to other RFIs involved in the execution of the transfer.

VIII.155 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 when added together exceeds $1,000, the verification requirements described in paragraphs VIII.123 and VIII.150 through VIII.151 apply.

VIII.156 POCR Regulation 11 requires each RFI that is a PSP to apply appropriate enhanced due diligence measures to transfers of funds presenting higher risks of ML/TF, including transfers involving:

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

VIII.157 Additional factors may cause a PSP to conduct enhanced due diligence on a transaction prior to authorising the transfer. These factors include, but are not limited to:

a) The PSP's risk tolerance and risk assessments;

b) The involvement of any agent or third-party service provider;
c) The nature of the transfer that has been requested, in the context of the accountholder's previous transactions and conduct.

VIII.158 Where a PSP becomes aware, in the course of processing a payment, that it is missing required information, or that the required information provided is meaningless or otherwise incomplete, the payee PSP must:

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

VIII.159 Additional detail concerning wire transfers and money transmission is set forth in paragraphs 5.30 through 5.35 and **Chapter 8: Wire Transfers**.

Refusing or terminating DAB

VIII.160 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 SAR to the FIA, in accordance with its obligations under POCA and ATFA.

VIII.161 Where an RFI conducting DAB decides that a business relationship must be terminated due to an inability to complete CDD, the RFI must take appropriate steps terminate the DAB or, as appropriate, not proceed with any proposed act, account, service, transaction or representation. Where there are no grounds for filing a SAR, any customer digital assets or other funds should be returned to the customer by transfer to a bank or other RFI, wherever possible, into the customer's account with a bank or other RFI from which the RFI originally received the digital assets or funds.

VIII.162 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.

Customer transactions or relationships involving cash or bearer instruments

VIII.163 Many digital assets are, or are highly similar to, cash or bearer instruments, which may be abused easily for criminal purposes. RFIs conducting DAB should be prepared to demonstrate that they have:

ii.

a) Evaluated the inherent ML/TF risks associated with their business;
b) Determined appropriate risk-mitigation measures; and
c) Documented relevant policies, procedures and controls that the RFI is in fact applying.

VIII.164 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. RFIs conducting DAB should establish similar norms and procedures with respect to the digital assets connected with their business.

VIII.165 Paragraphs 4.99 through 4.103 provide additional guidance on the use of bearer instruments.

Applicability of simplified due diligence to DAB

VIII.166 Simplified due diligence involves the application of reduced or simplified CDD measures in specified circumstances.

VIII.167 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.

VIII.168 Where a customer involves a person 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.

VIII.169 Where an RFI conducting DAB carries out an occasional transaction that amounts to less than $15,000, and that does not involve a transfer of funds, digital asset payment or wire transfer in an amount greater than $1,000, the RFI may consider whether it is required to verify the customer's identity. However, an RFI's risk assessment and, in particular, the higher ML/TF risks associated with cash-like and bearer instrument-like products and services may cause the RFI to determine that verification of a customer's identity is required to effectively mitigate risk. In addition, if there are features of a transaction or customer that suggest the RFI has entered into a business relationship, rather than an occasional transaction, verification is required. Additional information on occasional transactions and business relationships is set forth in paragraphs

VIII.96 through VIII.102.

VIII.170 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 DAB

VIII.171 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.

VIII.172 POCR 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.

VIII.173 In addition, enhanced due diligence must be applied in each of the following circumstances:

a) The agent, 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 (see paragraphs 5.18 through 5.19);
b) The customer or beneficial owner has not been physically present for identification purposes (see paragraph 5.25 through 5.29); and
c) The business relationship or occasional transaction involves a PEP (see paragraphs 5.96 through 5.116).

VIII.174 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.

VIII.175 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).

VIII.176 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 POCR 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 25% and understanding the voting rights of equity shares to ensure a complete understanding of the control structure of the entity involved.

VIII.177 Detailed information on enhanced due diligence, including in relation to new payment methods, is set forth in **Chapter 5: Non-Standard Customer Due Diligence Measures**.

VIII.178 Specific indicators of higher risk in DAB are discussed in greater detail in paragraphs VIII.241 through VIII.246.

International sanctions

VIII.179 RFIs conducting DAB should implement a sanctions compliance programme in line with the guidance set forth in **Chapter 6: International Sanctions**.

VIII.180 The Digital Asset Business (Prudential Standards) (Annual Return) Rules 2018 require each licensed DAB to submit an annual return that confirms or discloses, among other information:

a) Whether it screens clients to determine if they are subject to measures imposed under a Bermuda sanctions regime;
b) Whether it screens employees to determine if they are subject to measures imposed under a Bermuda sanctions regime;
c) Whether it has frozen any assets in the last 12 months under a Bermuda sanctions regime;
    i. If yes, the number of assets frozen
    ii. The licensed undertaking shall provide the following details for those asset freezes: group ID, name of the designated person as given on the consolidated list, name of the person/entity if

owned/controlled by a designated person and value of assets; and

d) The licensed undertaking shall include any additional information/comments, which might be relevant to the Authority in achieving its regulatory objectives in relation to the licensed undertaking.

VIII.181 RFIs should have in place processes for screening against the sanctions list customers, prospective customers and any third-party intermediaries seeking to introduce new business, and for performing background checks to identity information about a customer's association with financial or other crime, or with PEPs.

VIII.182 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.

VIII.183 RFIs must be aware that, in contrast to AML/ATF measures, which permit RFIs conducting DAB 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

VIII.184 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.

VIII.185 Ongoing monitoring in the context of DAB 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.

VIII.186 RFIs conducting DAB 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.

VIII.187 Failure to adequately monitor a customer's business relationship could expose

an RFI to abuse by criminals and may call into question the adequacy of the RFI's AML/ATF policies, procedures and controls and the integrity or fitness and properness of the RFI's management.

VIII.188 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 the 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 DAB; and
h) Adjusting risk profiles and risk assessments based on information reviewed.

VIII.189 Both at the time a customer is onboarded, and during ongoing monitoring, RFIs conducting DAB should evaluate:

a) Whether a customer's IP address correlates with other information the RFI holds on the customer, including nationality, residence and geolocation data;
b) Whether a customer's IP address is associated with a virtual private network (VPN) that may be used for the purpose of obscuring a customer's true location; and
c) Whether a customer's blockchain address, wallet address, public key or transaction history indicates any connection with a known or suspected mixer or tumbler service, the dark web or any other higher-risk person.

VIII.190 An RFI should require corporate customers to notify it of any material change to:

a) The nature of the customer's business;

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

VIII.191 It is the RFI's responsibility to maintain current information concerning the above.

VIII.192 In addition, each time a customer makes a payment into a money account in an amount of $15,000 or more, whether the payment is carried out in a single operation or several operations that appear to be linked, or otherwise contributes 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, digital assets or other difficult-to-trace payment methods could disguise the origin of the funds.

VIII.193 Ongoing monitoring must be carried out on a risk-sensitive basis. The inherent ML/TF risk levels associated with DAB should be considered when determining base-line 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.

VIII.194 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 DAB customers and the persons who own and control those customers. See paragraphs 7.11 through 7.14.

VIII.195 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.

VIII.196 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 paragraph VIII.89.

VIII.197 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.

VIII.198 Additional information regarding systems for monitoring and automated monitoring is set forth in paragraphs 7.15 through 7.21 of the general GN.

VIII.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, the persons who own, control and act on behalf of the customer and the business relationship with the RFI. See paragraph VIII.66.

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

Suspicious activity reporting

VIII.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.

VIII.202 RFIs conducting DAB 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.

VIII.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.

VIII.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 if the transaction or conduct is indeed suspicious or provides reasonable grounds for suspicion.

VIII.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.

VIII.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.

VIII.207 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.

VIII.208 Where, after evaluating an internal SAR, the reporting officer determines that there is knowledge, suspicion or reasonable grounds for suspicion that funds or assets are criminal property or that a person is involved in ML/TF, the reporting officer must promptly file an external SAR with the FIA.

VIII.209 The FIA no longer accepts any manually submitted SARs (including those faxed or emailed). The FIA accepts only those SARs that are submitted electronically via the goAML system, which is available at **www.fia.bm**.

VIII.210 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 SAR.

VIII.211 The FIA is located at 6th Floor, Strata 'G' Building, 30A Church Street, Hamilton HM11 and it can be contacted during office hours on telephone number (441) 292-3422, on fax number (441) 296-3422 or by email at info@fia.bm.

VIII.212 The Digital Asset Business (Prudential Standards) (Annual Return) Rules 2018 require each licensed DAB to submit an annual return that confirms, among other information:

a) That all employees are aware of the identity of the reporting officer and how to report suspicious activity;
b) Whether employees fully comply with all AML/ATF procedures in respect of customer identification, account monitoring, record keeping and reporting;
c) That employees are expected to remain vigilant to the possibility of ML/TF; and
d) Whether employees who violate POCR Regulations or laws and AML/ATF policies and procedures are subject to disciplinary action.

<u>Failure to report and tipping-off offenses</u>

VIII.213 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.

VIII.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 10 years on conviction on indictment, a fine up to an unlimited amount or both.

VIII.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 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.

VIII.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 POCR Regulations or any direction or licence condition imposed by the BMA.

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

VIII.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 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 a disclosure.

VIII.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.

VIII.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 offense. See paragraphs 9.82 through 9.88.

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

Employee training and awareness

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

VIII.223 RFIs must take appropriate measures to ensure that relevant employees, including, where appropriate, 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.

VIII.224 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; and
f) International sanctions (see paragraphs 6.52 through 6.54).

VIII.225 In a DAB context, training should enable relevant employees to:

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

VIII.226 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.

VIII.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 screening and compliance training programmes, as wellas 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.

VIII.228 The Digital Asset Business (Prudential Standards) (Annual Return) Rules 2018 require each licensed DAB to submit an annual return that confirms, among other information:

a) Whether it provides employees with training relating to ML/TF and, if yes, whether:
   i. ML/TF training is included in the induction program of new employees; and
   ii. The ML/TF training provided is specific to digital assets or is of general application;
b) The frequency that employees must undertake ML/TF training;
c) Whether adequate procedures or document information systems are in place to ensure relevant legal obligations are understood and practised by employees and adequate guidance and training are provided by it to employees;
d) Whether training programmes are designed to cover the AML/ATF risks of the licensed undertaking.
e) Whether it has an appropriate number of suitably trained employees and other resources necessary to implement and operate its AML/ATF programme;
f) That all employees are required to, at least annually, undertake training to ensure that their knowledge of AML/ATF laws, policies and procedures is current;
g) Whether employees are updated on ML schemes and typologies on a regular basis; and
h) That the compliance officer is trained in all applicable Proceeds of Crime laws in Bermuda and ML/TF risks arising from its business.

VIII.229 Detailed information on employee training and awareness is set forth in **Chapter 10: Employee Training and Awareness**.

Record-keeping

VIII.230 The record-keeping obligations of RFIs are governed primarily by POCR Regulations 15 and 16.

VIII.231 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.

VIII.232 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.

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

DABs as customers of other RFIs

VIII.234 In many instances, DABs 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 a DAB.

VIII.235 RFIs should not resort to the wholesale termination or exclusion of business relationships with DABs without first being informed by a proper risk assessment. Some financial institutions, perceiving DABs to be high-risk for ML/TF for the reasons set forth in paragraph VIII.70, have categorically terminated business relationships with DABs and refused to accept DABs as new customers. Such a systematic rejection of DABs 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.

VIII.236 Where an RFI reviewing a proposed or existing business relationship with a DAB 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 DAB, its owners, agents, policies and procedures, operations and customers.

VIII.237 RFIs should consider the degree to which a DAB 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 DAB. RFIs should take note that under Bermudian law, Bermudian DABs are RFIs subject to POCA, ATFA, POCA SEA, the POCR Regulations and these SSGN and general GN and are supervised by the BMA.

VIII.238 RFIs evaluating the commencement or continuation of a business relationship with a DAB 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 a principal in its own right, or an agent of another principal;
c) Length of time the business has operated;
d) Identity, experience and reputation of the business' beneficial owners and managers;
e) The business' formal AML/ATF policy statement (see paragraphs 1.31 through 1.37);
f) The business' AML/ATF policies, procedures and controls, including group-wide compliance programmes;
g) Names and contact information for the business' compliance officer and reporting officer (see paragraphs 1.38 through 1.50);
h) The business's internal and/or independent audits of the functioning of its AML/ATF policies, procedures and controls (see paragraphs 1.78 through 1.85);
i) The business' policies, procedures and controls for screening, onboarding, training and overseeing employees and agents;
j) The business' agent list;
k) The business' client profile;
l) The business' products and services profile;
m) Purpose of the DAB's proposed account(s) or business relationship and the type and level of anticipated account or other business activity; and
n) The business' assessment of the ML/TF risks it faces, and the mitigating measures it has put in place.

VIII.239 DABs 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 VIII.238, to ensure that the other RFI is able to meet its regulatory obligations and provide financial services to the DAB.

Risk factors for DABs

VIII.240 In addition to the non-exhaustive list of risk factors set forth in paragraph 2.37, RFIs conducting DAB should consider sector-specific risk factors, including those in paragraphs VIII.241 through VIII.246 below, 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.

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

a) A customer who offers false, fraudulent or fictitious 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 travelling unexplained distances to different locations of the RFI and/or its agents to conduct transactions;
l) A customer who frequently deposits and withdraws funds from its account for no apparent reason and/or the activity does not appear commensurate with its established risk profile;
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 criminal assets;
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 DAB or financial institution that

has been sanctioned by a respective national competent authority 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;

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;

bb) Regarding a customer engaging in a payment of digital assets or other funds:

i. A payer who is unwilling or unable to provide the required complete information;

ii. A payer for whom the complete information cannot be verified, where it is required to do so;

iii. A payer seeking to alter the customer information sent via the messaging system, for reasons that the PSP is not able to fully confirm as legitimate;

iv. A payer seeking to route the transaction through apparently unnecessary intermediary PSPs;

v. A payer seeking to ensure that the complete information does not reach all PSPs involved in the execution of the payment;

cc) A customer with a connection to online gambling; and/or

dd) A customer, agent, counterparty or intermediary that transacts with a known or suspected mixer or tumbler service, the dark web or any other higher-risk person.

VIII.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) A DAB transaction to, though or from a high-risk jurisdiction;

c) A non-face-to-face transaction initiated from a high-risk jurisdiction;

d) A DAB transaction linked to business in or through a high-risk jurisdiction;

e) DAB 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) A DAB 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.

VIII.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, international money transfers by mobile phone or the internet, and digital asset transfers and

other transactions with no geographic limits;

c) Products or services that have a very high or no transaction limit; and
d) Products or services that permit the exchange of cash for a negotiable instrument, such as a stored value card or a money order.

VIII.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 digital assets transfer, money transmission or other wire transfer 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) Large cash or bearer instrument transactions in circumstances where such a transaction would normally be made by cheque, banker's draft or non-digital asset wire transfer;
i) Transfers to the same person from different individuals or to different persons from the same individual with no reasonable explanation;
j) Transfers of funds that are not in line with the stated business activities of the customer;
k) Customers requesting transfers to or from overseas locations with instructions for payment to be made in cash or to blockchain addresses or wallet addresses about which insufficient information is known;
l) 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;
m) One-off or occasional transactions giving rise to suspicion;
n) Requests for digital assets or other securities or funds to be transferred to PEPs or higher-risk charities or other not-for-profit organisations not subject to effective supervision and monitoring;
o) A transfer with missing, meaningless or otherwise incomplete information;
p) A transfer of digital assets or other securities or funds in an amount greater than $1,000 to a non-account holder, including a blockchain address or wallet address that is not hosted by another RFI, particularly where no unique identifier accompanies the transfer;
q) A transfer for which a PSP knows or suspects that information provided by the payer PSP has been stripped or altered at any point in the payment chain;
r) A transfer for which there is evidence to suggest that a person other than the named payee is the intended final recipient; and
s) Transactions involving a known or suspected mixer or tumbler service, the dark web or any other higher-risk person.

VIII.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 the customer;
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;
c) A customer's use of an IP address that does not correlate with other information the RFI holds on the customer, including nationality, residence and geolocation data;
d) A customer's use of an IP address that is associated with a VPN that appears to be used for the purpose of obscuring the customer's true location; and
e) A customer's use of a blockchain address, wallet address or public key with a known or suspected connection with a mixer or tumbler service, the dark web or any other higher-risk person.

VIII.246 Third-party risk factors include, but are not limited to:

a) The involvement of any agent or other third party in carrying out any AML/ATF function in relation to a customer, including 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) Agents for which the RFI is unable to satisfactorily complete the steps set forth in paragraph VIII.142;
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;
n) Agents that conduct inconsistent or substandard data collection or record keeping;
o) Agents willing to accept false identification or identification records that contain false information, non-existent addresses that would be known to be non-existent to a person in that area, or phone numbers that are used as fillers;
p) Agents with a send-to-receive ratio that is not balanced, as compared with other agents in the locale, or that engage in transactions or activities indicative of complicity in criminal activity;
q) Agents whose ratio of questionable or anomalous customers to customers who are not questionable or anomalous is out of balance with the norm for comparable locations;
r) Agents who move money through RFI accounts in amounts not corresponding with the agent's DAB on behalf of the RFI;
s) Agents that are new businesses without an established operating history;
t) An agent that fails the RFI's transaction testing for compliance with the RFI's AML/ATF policies, procedures and controls; and
u) An agent with a known or suspected connection with a mixer or tumbler service, the dark web or any other higher-risk person.

***