Annex VIII

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

These sector-specific guidance notes should be read in conjunction with the main guidance notes for AML/ATF regulated financial institutions on anti-money laundering and anti-terrorist financing.

ANNEX VIII

SECTOR-SPECIFIC GUIDANCE NOTES FOR DIGITAL ASSET BUSINESS (DAB)

Contents

ANNEX VIII

SECTOR-SPECIFIC GUIDANCE NOTES FOR DIGITAL ASSET BUSINESS (DAB)

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). The guidelines herein are meant to supplement the 2016 Guidance Notes for AML/ATF Regulated Financial institutions on AML/ATF (hereinafter, "the main guidance notes"). These guidelines are to be considered and incorporated into a DABs AML compliance programme requirements for purposes of implementing a robust AML compliance programme in accordance with the AML/ATF obligations set forth under the AML/ATF Acts and Regulations of Bermuda that are specific to DAB, also known as virtual currency business.

VIII.2 Under Section 49(4)(a)(i) of the Proceeds of Crime Act and section 12A(2)(a)(i) of Anti-Terrorism (Financial and Other Measures) Act 2004 – the minister is given the power to make regulations to prescribe the classes of persons that should be subject to the regulations. Accordingly, regulation 4 of the Proceeds of Crime Regulations made under those provisions prescribe the persons to whom the regulations apply – hence all classes of persons in the financial services industry are together prescribed there as "*AML/ATF regulated financial institution*". Persons carrying on DAB within the meaning of Section 2(2) of the Digital Asset Business Act 2018 are prescribed as AML/ATF regulated financial institutions (RFIs).

VIII.3 With recent amendments (completed in July 2018) to the directions provisions, the term RFIs has been replaced by the term "relevant person" to empower the Minister to now also be able to issue such directions to non-financial regulated entities. Recent amendments have also made the definition in section 42A of POCA the sole substantive definition of the term for all of the other AML/ATF Acts and Regulations.

VIII.4 For the purposes of these guidance notes, the terms "AML/ATF relevant person should be understood to include persons conducting the DAB described in paragraph VIII.5. The term "digital asset business" should be understood to include any and all of the activities described in paragraph VIII.5.

VIII.5 Under Section 2(2) of the Digital Asset Business Act 2018, DAB means providing any or all of the following activities to the general public as a business:

i. <u>Issuing, selling or redeeming virtual coins, tokens or any other form of digital asset;</u>
This includes any business (incorporated or not) that provides these services to other businesses or individuals. This would include an Initial Coin Offering (ICO) business on behalf of customers, but not ICO activities to fund one's own company or project. An example of the former that will be subject to the Digital Asset Business Act 2018 is a company that operates a facility to assist its clients to launch ICOs. This includes assistance with coin or token design and administering the ICO process. An example of the latter that will not be subject to the Digital Asset Business Act 2018 is a company that wishes to issue its own ICO for its online gaming website or other business operations.

ii. <u>Payment service provider business utilising digital assets;</u>
The term Payment Service Provider (PSP) is a term used globally and is defined in the Proceeds of

Crime (Anti-Money Laundering and Anti-Terrorist Financing) Amendment Regulations 2010 as: "a person whose business includes the provision of services for the transfer of funds". The intention is to capture businesses involved in the transfer of digital assets.

iii. Operating an electronic exchange whereby digital assets of any type is, exchanged for cash or another digital asset;

Virtual currency exchanges are online exchanges that allow customers to buy and sell virtual currencies. Purchases and sales of digital assets can be made using either fiat currency (e.g., buying bitcoin using GBP or USD) or digital assets (e.g., buying bitcoin using another virtual currency such as ether). In addition to digital assets such as bitcoin and ether, digital asset exchanges may also facilitate the offer of new coins/tokens that are sold pursuant to ICOs/Initial Token Offerings (ITOs).

iv. Provision of digital assets custodial wallet services;

A digital assets wallet is a software programme that stores private and public keys and interacts with various blockchain to enable users to send and receive digital currency and monitor their balance. A digital asset itself is not actually "stored" in a wallet. Instead, a private key (secure digital code known only to the user and the wallet) is stored as proof of ownership of a public key (a public digital code connected to a certain amount of currency). By the wallet storing private and public keys, it allows the user to send and receive coins, and also acts as a personal ledger of transactions. The activity of developing wallet software or hardware is not within the scope of these AML/ATF obligations. Rather, those that provide custodial wallet services are within scope.

v. Digital assets services vendor;

This category is intended to capture any business providing specific digital asset related services to the public. This would include custodial and power of attorney rights over a customer's virtual currencies or market maker in digital asset activities.

VIII.6 By amending an order, the Minister may add categories of DAB in addition to those set forth in paragraph VIII.5.

VIII.7 RFIs conducting DAB should read these sector-specific guidance notes in conjunction with the main guidance notes for AML/ATF RFIs on AML/ATF. This annex supplements, but does not replace the main guidance notes.

VIII.8 Under Section 10 of the Digital Asset Business Act 2018 persons conducting DAB must obtain a licence from the Bermuda Monetary Authority (the Authority) prior to commencing business in Bermuda. However, section 11 of the Digital Asset Business Act 2018 provides for exemptions from licensure and sets forth the specific conditions where an institution carrying on DAB is not subject to the licensing requirements described in section 10. Such an institution is nonetheless an RFI subject to the AML/ATF requirements of Bermuda.

VIII.9 All RFIs must comply with the Acts and Regulations, and with the main AML/ATF guidance notes issued by the Authority.

VIII.10 Schedule 1, Section 2(2) of the Digital Asset Business Act 2018 sets forth that in determining whether an RFI is conducting its business in a prudent manner, the Authority will take into account any failure to comply, among other things, with:

- The Digital Asset Business Act 2018;
- The Proceeds of Crime Act 1997;

- The Anti-Terrorism (Financial and Other Measures) Act 2004;
- The Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 (Regulations); and
- International sanctions in effect in Bermuda.

VIII.11 Portions of this annex summarise or cross-reference relevant information that is contained in detail in the main guidance notes. The detailed information in the main guidance notes remains the authoritative guidance.

VIII.12 Portions of this annex include sector-specific information, such as risk factors that are particular to DAB. This sector-specific information should be considered as supplementary to the main guidance notes.

Status of the guidance

VIII.13 Approved by the Minister responsible for Justice, these guidance notes are issued by the Authority under Section 5(2) of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008 (SEA Act 2008); and in accordance with section 49M of the Proceeds of Crime Act 1997 (POCA 1997), and section 12O of the Anti-Terrorism (Financial and Other Measures) Act 2004 (ATFA 2004).

VIII.14 These guidance notes 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 are responsible for establishing, maintaining, and overseeing the RFI's risk-based management policies, procedures and controls for the prevention and detection of money laundering and terrorist financing (ML/TF).

VIII.15 The Court, or the Authority, as the case may be, in determining whether a person is in breach of a relevant provision of the Acts or Regulations, is required to consider whether a person has followed any relevant guidance issued by the Authority and approved by the Minister responsible for Justice. These requirements upon the Court or Authority are detailed in the provisions of Section 49M of POCA 1997, Regulation 19(2), Section 12O of, and paragraph 1(6) of Schedule 1 to, ATFA 2004 and Section 20(6) of the SEA Act 2008.

VIII.16 When a provision of the Acts or Regulations is directly described in the text of this guidance, the guidance notes use the term **"must"** to indicate that the provision is mandatory.

VIII.17 In other cases, the guidance herein uses the term **"should"** to indicate ways in which the requirements of the Acts or Regulations may be satisfied, while allowing for alternative means, provided that those alternatives effectively accomplish the same objectives.

VIII.18 Departures from this guidance, and the rationale for so doing, should be documented, and RFIs should stand prepared to justify departures to authorities such as the Bermuda Monetary Authority.

VIII.19 RFIs should be aware that under Section 16 of the Financial Intelligence Agency Act 2007, the Financial Intelligence Agency may, in the course of enquiring into a suspicious transaction or activity relating to money laundering or terrorist financing, serve a notice in writing on any person requiring the person to provide the Financial Intelligence Agency with such information as it may reasonably require for the purpose of its enquiry. In addition, under Section 63 of the Digital Asset Business Act 2018, the Authority may require a DAB under investigation for contravention of the Act, and any of

its controllers, officers, employees, agents, bankers, auditors, barristers or attorneys, to answer the Authority's questions, to provide documents to the Authority and to permit the Authority's entry into the business's premises.

VIII.20 Detailed information is set forth in the main guidance notes, beginning with the Preface.

Senior management responsibilities and internal controls

VIII.21 The AML/ATF responsibilities for senior management of an RFI conducting DAB are governed primarily by POCA 1997, SEA Act 2008, ATFA 2004, and the POCA Regulations 2008.

VIII.22 The AML/ATF internal control requirements for RFIs conducting DAB are governed primarily by Regulations 12, 16, 17A, 18 and 18A.

VIII.23 Regulation 19 provides that failure to comply with the requirements of specified Regulations is a criminal offence and carries with it significant penalties. On summary conviction, the penalty is a fine of up to $50,000. Where conviction occurs on indictment, penalties include a fine of up to $750,000, imprisonment for a term of two years, or both.

VIII.24 Section 20 of the SEA Act 2008 as amended in 2018 empowers the Authority to impose a penalty on an RFI of up to $10,000,000 for each failure to comply with specified Regulations. The amendments also provide for a number of disciplinary measures such as the power to issue directives, the power to impose restrictions on a licence, the power to issue a public censure, and the power to make prohibition orders, or take other disciplinary measures as set out in Chapter 4 of Part 3 of the SEA Act amongst others.

VIII.25 Under the relevant Acts and Regulations of Bermuda, senior management in all RFIs must:

- Ensure compliance with the Acts and Regulations;
- Identify, assess and effectively mitigate the ML/TF risks the RFI faces amongst its customers, products, services, transactions, delivery channels, outsourcing arrangements and geographic connections;
- Conduct an AML and Sanctions risk assessment and ensure that the risk assessment findings are maintained up to date;
- Appoint a Compliance Officer at the senior management level to oversee the establishment, maintenance and effectiveness of the RFI's AML/ATF policies, procedures and controls;
- Appoint a Reporting Officer to process client disclosures;
- Screen employees against high standards;
- Ensure that adequate resources are periodically trained and devoted to the RFI's AML/ATF policies, procedures and controls;
- Audit and periodically test the RFI's AML/ATF policies, procedures and controls for effectiveness and address any issues uncovered adequately and timely; and
- Recognise potential personal liability if legal obligations are not met.

VIII.26 RFIs must establish and maintain detailed risk-based policies, procedures and controls that are adequate and appropriate to forestall and prevent operations related to ML/TF. The risk-based approach measures are detailed in paragraph VIII.40 below

VIII.27 Under Section 12(6) (c) of the Digital Asset Business Act 2018, an RFI must include its AML/ATF policies and procedures with its application for a DAB licence.

VIII.28 Under Schedule 1, paragraph 5 (Consolidated supervision) of the Digital Asset Business Act 2018, a DAB must ensure that the structure of any group to which it belongs does not obstruct the conduct of effective consolidated supervision.

VIII.29 Where a Bermuda RFI conducting DAB has agents, branches, subsidiaries or representative offices located in a country or territory other than Bermuda, it must communicate its AML/ATF policies and procedures to all such entities, and must ensure that all such entities apply AML/ATF measures at least equivalent to those set out in the AML/ATF Bermuda Acts and Regulations.

VIII.30 Attempts to launder money through DAB may be carried out in several ways:

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

VIII.31 The majority of this annex addresses attempted money laundering by customers. Money laundering risks involving internal senior management, directors, managers, employees and agents are addressed via the screening for fit and proper requirements for DAB in paragraphs VIII.36 through VIII.39. Money laundering risks involving agents and other third parties are addressed in paragraphs VIII.159 through VIII.168.

VIII.32 Specific requirements for an RFI's detailed policies, procedures and controls are set forth in Chapters 2 through 11 of the main guidance notes.

VIII.33 Detailed information is set forth in Chapter 1: Senior Management Responsibilities and Internal Controls of the main guidance notes.

Links between digital asset business practices and AML/ATF policies, procedures and controls

VIII.34 An RFI's compliance with the Digital Asset Business Act 2018 achieves some of Bermuda's AML/ATF objectives. These objectives are also met in part through an RFI's compliance with the requirements, principles, standards and procedures set forth in guidance documents, including, but not limited to:

- Code of Practice - Digital Asset Business Act 2018
- Statement of Principles - Digital Asset Business Act 2018

VIII.35 The requirements of the AML/ATF Acts, Regulations and any additional guidance documents described in paragraph VIII.33 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 AML/ATF Bermuda Acts, Regulations and these guidance notes, whether as part of its existing business processes or through separate processes.

Ownership, management, employee and agent checks

VIII.36 To guard against potential money laundering involving owners, directors, managers, employees and agents of DABs, RFIs conducting money business should screen such persons against high standards in accordance with paragraphs 1.70 through 1.74 of the main guidance notes.

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

VIII.38 Where any screening is conducted by a third party, the RFI should have procedures to satisfy itself as to the effectiveness of the screening procedures the third party uses to ensure the competence and probity of each person subject to screening.

VIII.39 Working with agents, intermediaries and third party service providers that are licenced 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 in order to meet its screening obligations.

Risk-based approach for RFIs conducting digital asset business

VIII.40 RFIs conducting DAB must employ a risk-based approach in determining:

- Appropriate levels of customer due diligence (CDD) measures for different customer types;
- Proportionate risk-mitigation measures to prevent the abuse of the RFI's products, services, customer information, and delivery channels for ML/TF purposes;
- The scope and frequency of ongoing monitoring of a business relationship with a customer, and of transactions for which the RFI conducts CDD and screening against requisite sanctions/TF lists;
- The scope and frequency of conducting on-going/periodic reviews of customer files based on their assigned risk rating or score, and customer type; and
- Measures for monitoring, detecting and reporting suspicious activity to the appropriate authorities; as well as monitoring for activity that may increase a customer's risk profile.

VIII.41 The purpose of an RFI applying a risk-based approach is to balance the cost of AML/ATF compliance resources with a realistic assessment of the risk of the RFI being used in connection with ML/TF. A risk-based approach focuses resources and efforts where they are needed, and where they have the greatest impact in preventing and suppressing ML/TF.

VIII.42 By adopting a risk-based approach, competent authorities and financial institutions are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified;

VIII.43 Adopting a risk-based approach implies the adoption of a risk management process for dealing with money laundering and terrorist financing. This process encompasses recognising the existence of the risk(s) and developing strategies to manage and mitigate the identified risks.

VIII.44 The higher the risk an RFI faces from any particular combination of agent, customer, product, service, transaction, delivery channel or geographic connection, the stronger and/or more numerous the RFI's mitigation measures must be.

VIII.45 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.46 An RFI's assessment 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.47 RFIs must use a risk-based approach to determine whether each customer or business relationship entails a heightened level of ML/TF risk.

VIII.48 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.49 RFIs should document and be in a position to justify the basis on which they have assessed the level of risk associated with each particular combination of customer, product, service, transaction, delivery channel or geographic connection. This can be achieved by performing an assessment of a DABs AML and sanctions/terrorist financing risks, by way of conducting AML and sanctions risk assessments periodically. To do this effectively, a risk assessment methodology should be established.

VIII.50 When designing a new product or service or when venturing into the use of new technology platforms for delivery of new or existing products or services, an RFI conducting DAB must assess the risk of the product or service being used for ML/TF.

VIII.51 Managing the money laundering and terrorist financing risks arising from DAB is an ongoing process, not a one-off exercise.

VIII.52 RFIs must document the risk assessment procedures and controls, such as internal compliance audits, as this helps to keep them under regular review. There should be a process for monitoring whether such systems are working effectively, and how to improve them; for example, to reflect changes in the business environment, such as new product types or business models.

VIII.53 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 of the main guidance.

VIII.54 Managing the cybercrime activity that DABs are susceptible to is important and requires the DAB to assess the cyber risks it faces by establishing appropriate controls to reduce these risks. DABs should comply with the cybersecurity rules set forth in the Authority's Digital Asset Business (Cybersecurity) Rules 2018 and the Digital Asset Business Code of Practice.

ML/TF risks in the conduct of digital asset business

VIII.55 Using the risk-based approach, each RFI conducting DAB should determine the amount of ML/TF risk it will accept in pursuit of its business goals.

VIII.56 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.57 The DAB sector is often considered as posing a high risk of ML/TF. Criminals may be attracted to the sector because DAB:

- transactions are often fast, simple and irreversible;
- often involve cash or other digital asset products that do not necessarily rely upon other RFIs;
- is largely unregulated in many jurisdictions;
- may be cross-border, with a global reach;
- transactions in the case of certain DAB types are often one-off transactions, taking place outside of an established business relationship that could be otherwise more readily monitored for uncharacteristic behaviour;
- products and techniques could be used to facilitate anonymity, or to exploit a false identity; and
- activity involving agents, risks the agents not properly following appropriate AML/ATF policies, procedures and controls.

VIII.58 Although some DABs or digital assets may be abused by criminals for ML/TF purposes, not all DABs or digital assets are inherently high-risk for ML/TF.

VIII.59 The level of inherent risk associated with a particular DAB depends upon a number of factors, including, but not limited to:

- The size of the DAB;
- The products and services the business offers;
- The volume of activity being conducted through the business (domestically and/or globally);
- The extent to which branches and agents are involved in the business;
- The complexity of any payment chains used;
- The geographic areas in which the business operates; and
- The identity and geographic origin of the business's customers.

VIII.60 The level of inherent ML/TF risk may be lower where the business:

- 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;

- Is a digital asset transmitter that only remits virtual funds to domestic entities, particularly where both customer and recipients are RFIs and subject to AML/ATF regulations;
- Offers only a single line of digital asset business product or service; or
- Processes both sides of a transaction primarily for local residents.

VIII.61 The level of inherent ML/TF risk may be higher where the business:

- Deals significantly in cross-border transactions;
- Deals significantly in one-off transactions that are frequent and/or large in terms of currency amount;
- Offers several digital asset products or services;
- Is located in, or transacts with or through, a geographic area considered to be high risk for ML/TF or other criminal activity (see paragraph 5.19 of the main guidance notes);or
- Can be traced to, or from, mixing services[1], the dark web[2] or online gambling websites.

VIII.62 Even if a DAB offers only a single product or service, the business's risk assessment should identify categories of customers and transactions that are higher or lower risk within that single product or service. The DAB must also take note if the product has privacy (or enhanced anonymity) features and reflect this in the business risk assessment.

VIII.63 ML/TF risks associated with DAB can be reduced through the application of mitigation measures that are tailored to the risks the business identifies.

VIII.64 Examples of measures that may be used to mitigate ML/TF risk that an RFI has identified include, but are not limited to:

- Obtaining and verifying more customer information;
- Client transactions limits for the RFI's products and services;
- Geographic limits on the use of the RFI's products and services;
- Increased monitoring, including blockchain analysis and record-keeping; (monitoring systems should be searchable and record historical transactions using certain key metrics); and
- Segmentation of due diligence AML duties from control duties for independence/quality assurance purposes.

VIII.65 The mitigation measures noted in paragraph VIII.64 are detailed in the context of new payment methods in paragraphs 5.39 through 5.97 of the main guidance notes.

VIII.66 The results of an RFI's risk assessment must also be taken into account when the RFI determines and implements its AML/ATF programme including establishment and implementation of controls to address the aforementioned DAB ML/TF risks.

[1] Mixing services are depositories or facilities that allow a client to exchange digital assets. Accordingly a client deposits a digital asset with its associated historical footprint and after a period receives in exchange a different digital asset with a different footprint. This makes it difficult to track a transaction from its origin to final destination.

[2] The dark web is the part of the World Wide Web that can only be accessed through special software, such as The Onion Router ("TOR") network, increasing anonymity for users and website operators.

VIII.67 Specific factors of higher risk in DAB are discussed in detail in paragraphVIII.225 of this annex.

VIII.68 When identifying the ML/TF risk factors for a RFI's DAB, some of the questions which may inform your customer risk assessment include:

- Are your customers companies, partnerships, or trusts?
- What type of accounts are you holding for your customers? (i.e., are accounts linked to a verified bank account)?
- Will the customer only be transacting in digital assets therefore transacting strictly from a wallet?
- Do you undertake business in areas with highly transient populations?
- Is the customer base stable or does it have a high turnover?
- Do you act for international customers or customers you do not meet face-to-face?
- Do you accept business from abroad, particularly those based in, or have beneficial owners from countries with high levels of corruption (Transparency International corruption perception index), or where terrorist organisations operate?
- Do you act for entities that have a complex ownership structure or a cross-border element?
- Do you accept payments that are made to or received from third parties?
- How does the way the customer comes to the business affect the risk for:
    - Non face-to-face customers, and
    - Occasional transactions (in accordance with the guidelines in paragraph VIII.82 through VIII.88 of this guidance note), as opposed to ongoing business.
    - Does the pattern of behaviour, or changes to it, pose a risk?
- If you accept customer introductions from an agent or third party, have you accepted customers from this source before?

VIII.69 Whether or not a country is a high risk is not only determined by whether FATF has designated a country as high risk. Institutions must do their own due diligence to determine what other countries represent a high risk for ML, TF, and corruption. When determining the ML/TF risks the following factors will help to determine which customers should be looked at more carefully:

- Customers carrying out large one-off cash transactions;
- Customers that do not have a physical presence in the jurisdiction that they do business;
- Customers that are not licensed to do business in jurisdictions or areas where it is known that a license is required;
- Customers that are not local to the business;
- Overseas customers especially from a high-risk third country identified by the EU, FATF and CFATF;
- Complex business ownership structures with the potential for concealing beneficiaries;
- Customers carrying out frequent low-value transactions (see guidance on linked transactions paragraphs VIII.89 through VIII.93);

- Customers sending money or any form of digital assets to high-risk countries; and
- Customers who make use of mixing services or engage in transactions that can be tracked to the dark web or online gambling websites.

Customer Due Diligence (CDD)

VIII.70 RFIs conducting DAB must carry out CDD on their customers, as well as identify and conduct due diligence on the customers' beneficial owners. Therefore, DABs should be vigilant and ensure that they obtain sufficient information on each customer at account opening, as well as establish appropriate transaction monitoring rules in their systems to flag unexpected activity or activity that does not appear commensurate with a customer entity type or a customer's nature of the business/occupation.

VIII.71 See VIII.103 for the definition of a customer.

VIII.72 Detailed information on customer due diligence is set forth in chapter 3, (Overview of Due Diligence), Chapter 4 (Standard Due Diligence) and 5 (Non-Standard Due Diligence) of the main guidance notes, and paragraphs VIII.70 through VIII.168 of this annex.

VIII.73 Carrying out CDD allows RFIs to:

- Guard against impersonation/identity theft and other fraud by being satisfied that customers are who they say they are;
- Know whether a customer is acting on behalf of another;
- Identify any legal barriers (e.g. international sanctions) to providing the product or service requested;
- Maintain a sound basis for identifying, limiting and controlling AML/ATF risk exposure;
- Avoid committing offences under POCA and ATFA relating to ML/TF; and
- Assist law enforcement by providing information on DAB customers or activities being investigated.

VIII.74 CDD measures that must be documented in AML policies and procedures and carried out by the DAB include:

- Identifying and verifying the identity of the customer by establishing a customer identification program that sets forth the minimum requirements to be obtained for different customer types;
- Understanding the purpose and intended nature of the customer's business;
- Understanding the purpose and intended nature of the business relationship with the customer;
- Identifying the source of wealth and source of funds associated with the customer;
- Gathering information sufficient to understand the legal form, ownership structure and control structure of the customer under the domestic and/or foreign law governing the customer's formation, registration and operation;

- Identifying and verifying signatories, directors and other persons exercising control over the management of the customer or its relationship with the RFI;
- Identifying and taking reasonable measures to verify the identity of the beneficial owner(s) of the customer; and
- Updating the CDD information at appropriate times, utilising a risk-based approach.

VIII.75 The extent of CDD measures must be determined using a risk-based approach. Higher-risk situations require the application of enhanced due diligence (EDD) measures. Lower-risk situations may be eligible for the application of simplified due diligence (SDD) measures, provided that the RFI assesses the risk and determines it to be low and provided also that the RFI has no suspicion of ML or TF.

VIII.76 RFIs must be able to demonstrate to the Authority that the extent of their CDD measures and monitoring is appropriate in view of the risks of ML/TF.

VIII.77 Detailed information on CDD for private individuals is set forth in paragraphs 4.5 through 4.74 of the main guidance notes.

VIII.78 Detailed information on CDD for legal persons and other legal arrangements is set forth in paragraphs 4.75 through 4.135 of the main guidance notes.

Purpose and intended nature of the customer's transaction or business relationship with the RFI

VIII.79 The Regulations define a 'business relationship' as a business, professional or commercial relationship between an RFI and a customer, which, at the time contact is first made, the RFI expects to have an element of duration. A business relationship is also formed where the expectation of duration is not initially present, but develops over time. A relationship need not involve the RFI in an actual transaction; giving advice may often constitute the establishment of a business relationship.

VIII.80 An RFI must understand the purpose and intended nature of each proposed transaction or business relationship. In some instances the purpose and intended nature may appear self-evident. Nonetheless, using a risk-based approach, an RFI must obtain information that enables it to document and categorise the nature, purpose, size and complexity of the transaction or business relationship.

VIII.81 In many instances, a DAB customer will be a private individual. A DAB customer could also be a legal person or other legal arrangement which may pose a higher inherent risk for ML/TF. The DAB should maintain EDD procedures for addressing individuals (e.g. politically exposed persons (PEPs[3])). For customers that are not individuals, and particularly for customers that provide digital asset services, or are agents for DAB services, an RFI should collect information at account opening, including, but not limited to:

- The customer's purpose for the DAB relationship or transaction;
- The source of wealth and source of funds to be used in the DAB relationship or for the transaction(s) executed through the account;
- The anticipated type, volume, value, frequency, duration and nature of the activity that is likely to be undertaken through the DAB relationship or transaction;

[3] Refer to section 5.97 – 5.900 of the main guidance note for additional information PEPs

- The geographic connections of the customer and each beneficial owner, administrator, advisor, operator, employee, manager, director, agent or other person who is able to exercise significant power over the DAB relationship or occasional transaction;
- The means of payment (digital asset, cash, wire transfer, other means of payment);
- Whether there is any bearer arrangement, mail holding arrangement or care of (c/o) mail arrangement, and if so, the reasons for and details of the arrangement;
- Whether any payments are to be made to, though, or by third parties or agents, and if so, the reasons for and details of the request; and
- Whether there are any third party applications/tools that may be used to support or facilitate their transactions in any way.

The collection of the foregoing information and other information will assist the RFI in creating a customer risk profile at account opening. It will further assist the RFI in monitoring the customer's activity in the account against the established customer risk profile.

One-off transactions, occasional transactions and business relationships

VIII.82 To properly apply CDD, RFIs should distinguish between one-off transactions, occasional transactions, and transactions that take place as part of an ongoing business relationship.

VIII.83 The term 'one-off transaction' means a transaction carried out outside of a business relationship or unusual relative to customary business, regardless of the amount of the transaction.

VIII.84 The term 'occasional transaction' means a one-off transaction, amounting to $10,000 or more, whether the transaction is carried out in a single operation or several operations that appear to be linked. The term 'occasional transaction' also means any wire transfer or digital asset transmission carried out in an amount greater than $1,000. The values described in this paragraph refer to the net value of the transaction, not including the value of any commissions, fees or charges.

VIII.85 Many DABs carry out one-off transactions for customers that are outside of an ongoing business relationship. However, an RFI's introduction of a customer loyalty programme, relationship management tool or linkages with other financial services, when coupled with an agreement between the RFI and the customer, indicate that a business relationship has been formed.

VIII.86 Where a business relationship has been formed, an RFI must apply CDD measures, in accordance with its documented risk-based policies and procedures, to the relationship.

VIII.87 Where a one-off transaction is $1,000 or less and is assessed as being low-risk for ML/TF, and if neither ML nor TF are suspected in the circumstances, a relevant person is not required to apply the full CDD measures if they have collected sufficient evidence to be so satisfied or if they have sufficient prior knowledge of, an individual customer. See paragraphs VIII.109 through VIII.111.

VIII.88 Where a one-off transaction or business relationship involves more than $1,000 or is of a commercial nature, and particularly where a customer is a legal person or legal arrangement, CDD measures should be applied and recorded in accordance with these guidance notes.

Linked transactions monitoring

VIII.89 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 and regulatory reporting requirements, CDD requirements, or questions about the source of the funds.

VIII.90 RFIs should have transaction monitoring systems to identify and detect linked transactions, to apply EDD 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 must identify a series of transactions from several customers to the same recipient over a period of time.

VIII.91 An RFI's systems must be able to identify linked transactions that are conducted through any and all of the RFI's branches or agents.

VIII.92 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.93 As a matter of sound business practice, an RFIs transaction monitoring system should be capable of producing or facilitating the generation of a key performance indicator (KPI) and/or key risk indicator (KPI) metric reports. This includes the ability to detect linked transactions. This will help the RFI identity issues and/or trends for continued enhancements to its AML compliance programme.

Source of wealth and source of funds

VIII.94 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 to know or suspect that funds or assets are the proceeds of crime, or that a person is involved in money laundering or terrorist financing.

VIII.95 RFIs should make enquiries as to how a customer has acquired the wealth, whether in digital assets, securities, or any other assets, to be used with regard to the DAB relationship or transaction.

VIII.96 The extent of such enquiries should be made using a risk-based approach. Where a proposed one-off transaction is small and is assessed as low-risk for ML/TF, or where the source of wealth or funds is readily apparent, such enquiries may be limited in accordance with the RFI's AML/ATF policies, procedures and controls.

VIII.97 RFIs should 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.98 More frequent and thorough source of wealth measures should be taken if the customer is a PEP that presents a higher risk.

VIII.99 Additional information on the source of funds and source of wealth is set forth in paragraphs 5.110 through 5.113 of the main guidance.

Definition of a customer in a DAB context

VIII.100 An RFI's customer is generally a private individual, legal person, trust or other legal arrangement with or for whom a business relationship is established, or with or for whom a one-off transaction is carried out. A given DAB relationship or transaction may have more than one person who is a customer.

VIII.101 A customer that is not a private individual generally involves a number of individuals, 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 itself, but also the individuals who comprise the customer entity and its relationship with the RFI.

VIII.102 Where a one-off transaction or business relationship involves multiple parties, such as when a digital asset is being transmitted with the involvement of one or more agents, any agent may also be a customer.

VIII.103 For the purposes of these guidance notes, a customer includes each of the following:

- Each private individual, legal person, trust or other legal arrangement that is or comprises a **customer** seeking a digital asset business product or service;
- Each **agent** involved in a business relationship or one-off transaction; and
- Each **beneficial owner** of a customer.

VIII.104 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.105 Where a customer is an agent[4]acting on behalf of a principal who is a third person, 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. RFIs contemplating reliance on a third party for the purposes of applying CDD measures should have regard to paragraphs 5.118 through 5.148 of the main guidance notes.

VIII.106 Additional information on the meaning of customer, business relationship and occasional transaction and on identifying and verifying individuals, 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.107 RFIs must consider as beneficial owners those persons who own or control a customer or its management, directly or indirectly, including through any bearer or nominee arrangement (both shareholders and directors). The definition of a beneficial owner can be found in section 98C of the Companies Act 1981.

[4] Guidance around agent networks specifically, and other third parties is detailed in paragraphs VIII.159 to 168.

VIII.108 Information on the identification and verification of beneficial owners is set forth in Regulation 3 and Chapter 4: Standard Customer Due Diligence Measures.

Obtaining and verifying customer identification information

VIII.109 RFIs must utilise a risk-based approach to determine the extent of identity information or evidence it requests and verifies. In making its determinations about the ML/TF risk associated with a transaction, an RFI should take into account factors such as:

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

VIII.110 A person who is a customer in the DAB context may be an individual, legal person, trust or other legal arrangement. For each type of customer, RFIs should follow the identification and verification requirements in Chapter 4: Standard Customer Due Diligence Measures, as supplemented by any relevant Annexes.

VIII.111 Evidence of identity may be in documentary or electronic form. An appropriate record of the steps taken, and copies or records of the evidence obtained to identify the customer, must be kept as per the record-keeping portion of this guidance.

Standard identification requirements for private individuals

VIII.112 Where a customer forms a business relationship with an RFI, the RFI must obtain and verify identification information for that person, at a minimum, using standard identification requirements set forth below.

VIII.113 Where the customer has not formed a business relationship with the RFI and is instead engaging in a one-off transaction, the customer identification requirements may differ on the basis of the type of transaction, the size of the transaction, and whether the transaction is linked with other transactions.

VIII.114 Where a one-off transaction is an occasional transaction, that is a transaction in amount of $10,000 or more, or a wire transfer or money transmission, or digital asset transmission, in an amount greater than $1,000, whether carried out in a single operation or several operations which appear to be linked, an RFI must apply, at a minimum, the standard CDD measures.

VIII.115 An RFI fulfils the standard identification requirements by obtaining a private individual's:

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

VIII.116 In addition, an RFI fulfils the standard identification for private individuals, by verifying the following using appropriate documentary or electronic means:

- Full legal name;
- Principal residential address; and
- Date of birth.

Simplified identification requirements for private individuals

VIII.117 Where the risks of money laundering or terrorist financing are lower and there is no suspicion of either ML or TF, DABs are allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold);
- Reducing the frequency of customer identification updates;
- Reducing the degree of ongoing monitoring and scrutinising transactions, based on a reasonable monetary threshold; and
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

VIII.118 Any application of simplified identification requirements must be made only after conducting a risk assessment and arriving at a reasonable conclusion that the category of one-off transactions to which the simplified requirements are to be applied is low risk for ML/TF.

VIII.119 Where an RFI carries out any wire transfer or other money transmissions, or digital asset transmission, on behalf of its customer in an amount greater than $1,000, the RFI must apply the standard CDD measures even if such a transaction is an occasional transaction.

VIII.120 RFIs should nonetheless determine whether any of the DAB activities listed in paragraph VIII.5, whether alone or in combination with another product or service the RFI offers, do in fact involve a

wire transfer or money transmission, or digital asset transmission that would require the application of standard CDD measures.

VIII.121 Where an RFI conducting DAB has confirmed that a particular one-off transaction in an amount less than $10,000 does not involve a wire transfer or money transmission or digital asset transmission, and that the transaction and customer are **low-risk** for ML/TF and there is no suspicion of ML or TF, the RFI is not automatically required to conduct full CDD for the customer.

VIII.122 Nonetheless, RFIs should obtain and verify the identity of customers for all DAB transactions unless the RFI has documented a probability that the application of standard CDD requirements will drive a class of legitimate customers to transact outside of the regulated financial sector, or will cause a class of legitimate customers to be unable to access the service in question by any means.

VIII.123 Bearing in mind the above, an RFI's AML/ATF risk assessment may inform the RFI's establishment of transactional thresholds, customer profiles, or other criteria to establish customer identification or monitoring procedures under the RFI's AML/ATF policies, procedures and controls.

Obtaining and verifying beneficial owner information

VIII.124 RFIs applying standard CDD requirements must obtain and verify identification information for the beneficial owners of any customer, in accordance with the requirements set forth under section 4 of the main guidance notes, *Standard Customer Due Diligence Measures*.

VIII.125 A beneficial owner is normally an individual who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted.

VIII.126 In respect of customers who are private individuals, the customer himself is the beneficial owner, unless there are features of the transaction or surrounding circumstances that indicate otherwise.

VIII.127 Where there is a reason to believe that a person is not acting on his own behalf, an RFI should make appropriate enquiries to identify and verify the customer and beneficial owner. Where a private individual is fronting for another private individual who is the beneficial owner, the RFI should obtain the same information about that beneficial owner as it would for a customer. For further guidance regarding a person acting under power of attorney or as an executor or personal representative, see paragraphs 4.45 to 4.47 of the main guidance.

VIII.128 Where control or ownership is held by another legal person or legal arrangement, RFIs should consider as a beneficial owner each private individual who ultimately controls or owns that other legal person or legal arrangement.

VIII.129 Additional information on the identification and verification of beneficial owners, including beneficial owners of customers that are legal persons, trusts or other legal arrangements, is set forth in Regulation 3, Chapter 4: Standard Customer Due Diligence Measures, and Annex I: Sector-Specific Guidance Notes for Trust Business

Timing of customer due diligence

VIII.130 An RFI must apply risk-based CDD measures when it:

- Establishes a business relationship at account opening;

- Carries out an occasional transaction[5] in an amount of $10,000 or more, whether the transaction is carried out in a single operation or several operations which appear to be linked;
- Carries out any wire transfer or digital asset transmission in an amount of $1,000 or more (see Chapter 8: Wire Transfers);
- Suspects money laundering or terrorist financing;
- Doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification; or
- Has committed to doing so under the RFI's risk-based AML/ATF policies, procedures and controls, for example, when the RFI conducts a one-off transaction in an amount below $10,000 that is not a wire transfer or money transmission.

VIII.131 Where the product or service is a one-off transaction[6] amounting to not less than $10,000 and the transaction does not involve a wire transfer or money transmission, the RFI should apply CDD measures at the time the one-off transaction is entered into.

VIII.132 Where a customer who has carried out a one-off transaction amounting to less than $10,000 requests a future or ongoing service, or returns to carry out further transactions, the RFI should consider whether the transactions are linked, or whether it is entering into a business relationship requiring CDD measures.

VIII.133 Verification should take place:

- Before the RFI accepts a new customer;
- Before the RFI provides any service as part of a business relationship;
- Before the RFI carries out any occasional transaction; and
- 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.134 Detailed information on the timing of CDD measures is set forth in Chapter 3: Overview of Customer Due Diligence of the main guidance notes.

Customer transactions involving cash or bearer instruments

VIII.135 Many RFIs conducting DAB handle cash or bearer instruments, which may easily be abused for criminal purposes. Due to the higher inherent risk of ML/TF where cash or bearer instruments are involved, RFIs must ensure that the inherent risks are identified, evaluated and mitigated using appropriate AML/ATF measures.

VIII.136 While some transactions below $10,000 may not automatically require the application of standard CDD, an RFI's AML/ATF risk assessment may determine that the use of cash or bearer instruments in such transactions, or the involvement of other higher risk factors requires the RFI to conduct CDD.

[5] More information around occasional transactions are detailed earlier on in this guidance note. See paragraphs VIII.82 to VIII.88.
[6] Information on one-off transactions is detailed earlier on in this guidance note. See paragraphs VIII.82 to VIII.88.

VIII.137 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.

VIII.138 Paragraphs 4.97 through 4.101 provide additional guidance on the use of bearer instruments.

Applicability of simplified due diligence to digital asset business

VIII.139 Simplified due diligence (SDD) involves the application of reduced or simplified CDD measures in specified circumstances.

VIII.140 RFIs may consider applying reduced or SDD measures only where the risk assessment process results in a finding of lower than standard risk and where there is no suspicion of ML or TF in the particular circumstances.

VIII.141 Paragraphs VIII.117 through VIII.123 set forth that in the context of DAB, a one-off transaction in an amount lower than $10,000 that does not involve a wire transfer or money transmission may be eligible for simplified CDD. However, paragraphs VIII.135 through VIII.138 clarify that an RFI's risk assessment may cause the RFI to conduct CDD on occasional transactions that involve cash, bearer instruments or other higher-risk criteria where those risks are not effectively mitigated through other means.

VIII.142 Where a transaction involves an entity for which SDD is appropriate, RFIs must nonetheless adhere to the guidance notes in identifying and verifying signatories and other persons connected with the customer.

VIII.143 Detailed information on the applicability of SDD is set forth in paragraphs 3.17 and 5.1 through 5.14.

Refusing or terminating digital asset business

VIII.144 If for any reason an RFI is unable to complete CDD measures in relation to a customer, Regulation 9 of the Bermuda Proceeds of Crime (Anti-money laundering and Anti-terrorist financing) Regulations 2008 establishes that the RFI must:

- In the case of a proposed business relationship or transaction, not establish that business relationship or open an account and not carry out that transaction with or on behalf of the customer;
- In the case of an existing business relationship, terminate that business relationship with the customer; and
- Consider whether the RFI is required to make a Suspicious Activity Report to the Financial Intelligence Agency (FIA), in accordance with its obligations under POCA 1997 and ATFA 2004.

VIII.145 Regardless of whether an RFI is an originating, intermediary, or beneficiary RFI of any wire transfer or money transmission, it must have effective risk-based policies and procedures for

determining when to execute, reject, or suspend the wire transfer or money transmission, or digital asset transmission, and the capacity to timely effectuate any rejection or suspension.

VIII.146 Where an RFI declines or terminates business that it knows is, or suspects might be, criminal in intent or origin, the RFI should refrain from referring such declined business to another person.

Enhanced due diligence for digital asset business

VIII.147 Enhanced due diligence (EDD) is the application of additional CDD measures where necessary to ensure that the measures in place are commensurate with higher ML/TF risks.

VIII.148 Regulation 11 of the Bermuda Proceeds of Crime (anti-money laundering and anti-terrorist financing) Regulations 2008, requires RFIs to apply EDD in all situations where a customer or the products, services, delivery channels or geographic connections, with which the customer engages, present a high risk of money laundering or terrorist financing. Specifically, a DAB's EDD procedures should be risk-based and tailored to account for unique risks presented by its customers, such as risks presented by certain customer types (e.g., individuals, agents, digital asset transmitters, specifically when unregulated, etc.), customer attributes (e.g. customers located in a high risk jurisdictions, cash-based or cash-intensive businesses etc. Politically Exposed Persons (PEPs)), and customer activity (e.g. wire transfers). More information on customer attributes to consider is contained in paragraphs VIII.149 to VIII.152 and information on the EDD measures that DABs can apply is outlined in paragraphs VIII.154 to VIII.157.

VIII.149 In the context of DAB, the involvement of agents in the provision of an RFI's services may require an RFI to apply enhanced due diligence to its own agent network.

VIII.150 In addition, the use of new payment methods[7] in the context of DAB may require an RFI to apply EDD. Risk factors common to many new payment methods include, but are not limited to:

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

VIII.151 Additional information on EDD for new payment methods is set forth in paragraphs 5.37 through 5.96 of the main guidance note.

VIII.152 Amongst other circumstances, EDD must be applied in each of the following circumstances:

[7]Guidance around new payment methods (NPM), including their risk factors and mitigation measures can be found in paragraph 5.37 through paragraph 5.94 in the main guidance notes.

- The agent, business relationship or one-off transaction has a connection with a country or territory that represents a higher risk of money laundering, corruption, terrorist financing or being subject to international sanctions (see paragraphs 5.19 through 5.20);
- The customer or beneficial owner has not been physically present for identification purposes (see paragraph 5.26 through 5.30) of the main guidance notes and
- The agent, business relationship or occasional transaction involves a PEP (see paragraphs 5.97 through 5.117 of the main guidance notes).

VIII.153 Where an RFI determines that EDD measures are necessary, it must apply specific and adequate measures to compensate for the higher risk of money laundering.

VIII.154 In selecting the appropriate additional measures to be applied, RFIs should consider obtaining additional information and approvals, including one or more of the following:

- Additional information on the agent or customer, such as the persons who comprise, own and control the agent or customer, the nature of the agent or customer's business, volume of assets and information available through public databases;
- Additional information on the nature and purpose of the business relationship (see paragraphs 4.1 through 4.4 of the main guidance notes);
- Additional information on the source of wealth and source of funds of the customer (see paragraphs 5.110 through 5.113 of the main guidance notes);
- Additional information on the reasons for planned or completed transactions; and
- Approval of the RFI's senior management to commence or continue the agency relationship, customer business relationship, or one-off transaction (see paragraph 5.109 of the main guidance notes).

VIII.155 In addition, RFIs should consider applying additional measures, such as:

- Updating more frequently the identification and verification data for the agent or customer, its beneficial owner(s), and any other persons who own or may exercise control over the agent or customer; and
- Conducting enhanced monitoring of the agent relationship or customer business relationship by increasing the number and frequency of controls applied and by identifying patterns of activity requiring further examination.

VIII.156 Additional mitigation measures are set forth in paragraphs VIII.64 herein, and 5.37 through 5.96 in the main guidance note.

VIII.157 Detailed information on enhanced due diligence is set forth in Chapter 5: Non-Standard Customer Due Diligence Measures of the main guidance note.

VIII.158 Specific indicators of higher risk in DAB are discussed in greater detail in paragraphs VIII.225 through VIII.231 of this annex.

Agent networks and other third parties

VIII.159 Where an RFI's DAB involves an agent network, or other third parties, RFIs 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. The process for obtaining and reviewing this information should be outlined in the RFI's policies and procedures.

VIII.160 RFIs should require agents and other third parties to demonstrate that they are examined for compliance with appropriate AML/ATF obligations.

VIII.161 An RFI may have a range of contractual relationships with agents or third parties. Some agents may be considered as an integral part of the RFI, and therefore directly subject to the RFI's AML/ATF policies, procedures and controls. Other agents may be considered wholly separate entities upon which the RFI seeks to rely for purposes of AML/ATF. Still other agents may be most accurately considered customers entering into a business relationship with the RFI, for which appropriate CDD must be conducted. Each RFI must ensure that this range of possible relationships does not prevent the effective implementation of appropriate AML/ATF controls at all levels of any agency structure or multiparty payment chain.

VIII.162 RFIs that provide services with the involvement of other parties must determine the distribution of AML/ATF responsibilities between the parties.

VIII.163 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:

<u>Prior to onboarding the agent</u>

- Require the agent to demonstrate that it is properly licensed, registered and supervised for compliance with appropriate AML/ATF obligations;
- Require the agent to provide the information set forth in paragraph VIII.168 of this annex, which the RFI must include in its agent list;
- Conduct a beneficial ownership assessment, including fit-and-proper testing and a review of negative media;
- Conduct a criminal background check of the agent's ownership, management and relevant employees;
- Verify any required compliance credentials of relevant employees; and
- Review the agent's AML/ATF policies, procedures and controls, and ensure that the distribution of AML/ATF responsibilities is in line with the requirements of these guidance notes.

<u>After onboarding the agent</u>

- Train the agent on the RFI's AML/ATF policies, procedures and controls;
- Conduct ongoing monitoring of transactions and business relationships involving the agent;
- Conduct ongoing monitoring and testing of the agent's compliance with the relevant AML/ATF policies, procedures and controls;
- Consider whether on-site visits and/or testing is merited;

- Take prompt corrective action as needed, including filing Suspicious Activity Reports about the agent where appropriate; and
- Terminate the relationship where appropriate.

VIII.164 Where an RFI relies upon 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, whether or not 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.165 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.166 Paragraphs 5.118 through 5.148 of the main guidance note sets forth the circumstances in which reliance on a third party is permissible. Paragraphs 3.22 through 3.24 provide additional relevant guidance. In any reliance situation, however, the relying RFI retains responsibility for any failure to comply with a requirement of the regulations, as this responsibility cannot be delegated.

VIII.167 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 supervises for compliance with, an appropriate AML/ATF regulatory regime.

VIII.168 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 Authority upon request. Such an agent list should include, at a minimum:

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

Money or digital asset transmission and wire transfers

The paragraphs within this section contain guidance around specific controls that RFIs should establish in order to mitigate ML/TF risks associated with various kinds of money or digital asset transmission/wire transfer activity that can be transacted through or within their institution.

VIII.169 In the context of the Digital Asset Business Act 2018, any digital asset transmission by a PSP business will be viewed as a wire transfer and subject to the rules for wire transfers set forth in

Regulations 21 through 31 of the the Bermuda Proceeds of Crime (anti-money laundering and anti-terrorist financing) Regulations 2008, the Bermuda Monetary Authority Guidance for Wire Transfers 2010 and Chapter 8: Wire Transfers. The 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.170 RFIs conducting wire transfers or money/digital asset transmissions should ensure that the identity of the payee is accurate and verified for any cross-border transfer of funds over $1,000, and for any cross-border transaction that is carried out in several operations that appear to be linked and together exceed $1,000.

VIII.171 Where the payee has a business relationship with the payee RFI, the payee's identity is accurate and verified if the information has been satisfactorily obtained and verified in accordance with the regulations and these guidance notes. However, a number of factors may cause an RFI to conduct additional CDD on a customer prior to disbursing any funds from the transfer. These factors include but are not limited to the RFI's risk tolerance and risk assessments, the involvement of any agent or third party service provider, the involvement of higher-risk persons or jurisdictions, and the particular nature of the transfer that has been received in the context of the accountholder's previous transactions and conduct.

VIII.172 Where the payer does not have a business relationship with the RFI and the wire transfer or money/digital asset transmission exceeds $1,000, the payer RFI must satisfactorily obtain and verify the identity and address of the payer prior to executing the transaction. Where the address is substituted with a payer's date and place of birth, customer identification number or national identity number, that information must also be verified. In addition, the RFI must verify the complete information where a transaction is carried out in several operations that appear to be linked and together exceed $1,000.

VIII.173 Where the payer does not have a business relationship with the RFI and the wire transfer or money/digital asset 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, customer identification number or 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. Where a transaction is carried out in several operations that appear to be linked and together exceed $1,000, the verification requirements described in paragraph VIII.172 apply.

VIII.174 Additional information concerning wire transfers and money transmission is set forth in Chapter 8: Wire Transfers. Such should also, in principle, be applied to digital asset transmission.

International sanctions

VIII.175 RFIs conducting DAB should implement a sanctions compliance programme in line with the guidance set forth in Chapter 6: International Sanctions of the main guidance note.

VIII.176 RFIs should determine whether any persons connected with a customer, and the individuals behind any such persons that are legal entities, trusts or other legal arrangements, are sanctions targets by screening them against the requisite sanctions lists referred to in chapter 6 of the main guidance notes. Specifically, the details of each sanctions regime in effect in Bermuda is contained in paragraph 6.20 of the chapter.

VIII.177 RFIs must be aware that, in contrast to AML/ATF measures, which permit RFIs some flexibility in setting their own timetables for verifying and updating CDD information, an RFI risks breaching a sanctions obligation as soon as a person, entity or good is listed under a sanctions regime in effect in Bermuda. In addition, whereas an RFI may choose to transact with a higher-risk individual or entity, it may not transact with any individual or entity subject to the Bermuda sanctions regime without first applying for and obtaining an appropriate licence.

VIII.178 Additional information concerning international sanctions, including information around penalties for non-compliance, asset freezing and other restrictions, and the establishment of appropriate sanctions policies and procedures, are set forth in Chapter 6: International Sanctions of the main guidance note.

On-going monitoring

VIII.179 Regulations 6(3), 7, 11(4)(c), 13(4), 16 and 18[8] require RFIs to conduct ongoing monitoring of a business relationship with a customer, and of transactions for which the RFI conducts CDD.

VIII.180 Ongoing monitoring in the context of DAB supports several objectives:

- Maintaining a proper understanding of a customer's identity and activities;
- Ensuring that CDD documents and other records are accurate and up-to-date and that customer risks are periodically evaluated utilising a risk-based approach, by way of conducting periodic reviews of customer files based on their risk classification;
- Providing accurate inputs for the RFI's ongoing risk assessment processes;
- Testing the outcomes of the RFI's ongoing risk assessment processes;
- Detecting and scrutinising unusual or suspicious conduct in relation to a customer by way of transaction monitoring; and
- Evaluating the compliance of agents with the RFI's AML/ATF policies, procedures and controls.
- Failure to adequately monitor transactions or business relationships, for example by failing to put in place effective systems to identify linked transactions, 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.181 RFIs should determine the scope and frequency of ongoing monitoring using a risk-based approach. RFIs should direct greater monitoring resources toward those products, services and business relationships presenting a higher risk of money laundering or terrorist financing than to those presenting a lower risk.

VIII.182 Transaction monitoring (TM) guidelines can include:

- A DAB ensuring that appropriate AML scenarios/rules are incorporated into its TM system to identify potentially suspicious activity
- Ensuring that the TM rules/scenarios are appropriately configured to address any Bermuda AML regulatory reporting requirements within any required timeframes

[8] In accordance with the Bermuda Proceeds of Crime (anti-money laundering and anti-terrorist financing) Regulations 2008

- Consideration of TM systems that generate reports, and how they will be utilised
- DABs needing to establish and implement effective TM procedures, including guidance around reviewing and ruling on TM alerts generated from the system
- DABs need to establish and implement procedures around conducting model validation/system effectiveness reviews periodically so as to ensure that TM and sanctions filtering systems are operating as intended
- Leveraging the results of any risk assessments performed, as well as any pertinent AML industry guidance to adjust TM rules/scenarios accordingly

VIII.183 Periodic file reviews can include:

- The need to establish a risk-based periodic review approach e.g. High risk accounts to be reviewed every 6 – 12 months, Medium every 1.5 – 2 years, and Low 2.5 – 3 years
- Establishing procedures around the KYC review process for conducting these reviews is based on a customer's risk classification (in our experience, some institutions will conduct a manual sampling of transactions as part of this process), as well as criteria around factors for downgrading or upgrading a customer file, requisite approvals that need to take place for adjustments made to these risk ratings during the review, and any exceptions that a DAB chooses to employ as part of its process
- The guidelines referenced in this section can also be tailored to the above, as necessary.

VIII.184 RFIs must be able to demonstrate to their supervisory authority that the extent of their CDD measures and ongoing monitoring is appropriate in view of the risks of money laundering and terrorist financing.

VIII.185 With respect to the customer, RFIs should consider:

- The nature, amount and frequency of the transactions;
- Geographic connections (see paragraph 2.48);
- Whether the customer is known to use other products and services;
- Whether the customer can be categorised according to activity or turnover;
- Whether the customer's conduct falls outside any norms established for any categories identified; and
- Whether the customer presents a higher than standard risk for money laundering or terrorist financing.

VIII.186 Ongoing monitoring includes:

- Scrutinising one-off transactions and business relationships to ensure that the transactions and business conduct are consistent with the RFI's knowledge of the customer and his risk profile, the product or service and its risk profile, and the RFI's risk-based policies, procedures and controls;
- Investigating the background and purpose of all linked, complex or unusually large transactions, and unusual patterns of transactions which have no apparent economic or lawful purpose, and recording in writing the findings of the investigation; and

- Reviewing existing documents, data and information to ensure that they are up-to-date, adequate and relevant for the purpose of applying CDD measures.

VIII.187 Ongoing monitoring must be carried out on a risk-sensitive basis. Higher-risk customers and business relationships, including those involving agents, must be subjected to EDD and more frequent and/or intensive ongoing monitoring.

VIII.188 Bearing in mind that some criminal activity may be so widespread as to appear to be the norm, RFIs should establish norms for lawful one-off transactions and conduct in relation to DAB customers, including norms for activities involving cash or bearer instruments. See paragraphs 7.11 through 7.14.

VIII.189 Once an RFI has established norms for lawful one-off transactions and conduct, it must monitor any business relationship, transactions, patterns of transactions and conduct by customers, and the persons who own and control those customers, to identify transactions and conduct falling outside of the norm.

VIII.190 Monitoring may take place both in real time and after the event, and it may be manual or automated. Irrespective, any system of monitoring should ensure at its core that:

- Customers, transactions and conduct are flagged in exception reports for further examination;
- The exception reports are reviewed promptly by the appropriate person(s); and
- Appropriate and proportionate action is taken to reduce the possibility of money laundering or terrorist financing occurring without detection.

VIII.191 An RFI should calibrate its monitoring systems to identify for review all higher-risk activity, including, but not limited to:

- Transactions or conduct falling outside of the expected norm for a customer, product or service;
- All complex or unusually large transactions and unusual patterns of transactions which have no apparent economic or lawful purpose;
- Transactions for which the customer has not been physically present for identification purposes (see paragraph 5.26 through 5.30); of the main guidance;
- Business involving a correspondent banking relationship (see paragraph 5.148 of the main guidance notes);
- A business relationship or occasional transaction involving a PEP (see paragraphs 5.97 through 5.117 of the main guidance notes);
- A business relationship or occasional transaction that has a connection with a country or territory that represents a higher risk of money laundering, corruption, terrorist financing or being subject to international sanctions (see paragraph 5.19 of the main guidance notes);
- Transactions that may favour anonymity, including new payment methods (see paragraphs 5.37 through 5.96 of the main guidance notes), and those involving dark web/mixing/tumbler services; and
- Transactions with regard to which an agent of the RFI has not followed the requisite AML/ATF policies, procedures and controls.

VIII.192 Where an RFI accepts higher-risk business, it must ensure that it has the capacity and expertise to effectively conduct on-going monitoring of the customer, the products and services being offered, and any business relationships the RFI forms, including those involving agents. See paragraph VIII.46.

VIII.193 Additional information on ongoing monitoring is set forth in Chapter 7: On-Going Monitoring of the main guidance.

Suspicious activity reporting

VIII.194 The suspicious activity reporting requirements for RFIs are governed primarily by Sections 43 through 48 of POCA 1997, Schedule 1 of ATFA 2004, and Regulations 16 and 17.

VIII.195 RFIs conducting DAB must put in place appropriate policies and procedures to ensure that knowledge, suspicion and reasonable grounds to know or suspect that funds or assets are the proceeds of crime, or that a person is involved in money laundering or terrorist financing, are identified, enquired into, documented and reported.

VIII.196 The definitions of knowledge, suspicion and reasonable grounds to know or suspect are set forth in paragraphs 9.6 through 9.10 of the main guidance.

VIII.197 Many customers will, for perfectly good reasons, have an erratic pattern of transactions or activity. A transaction or activity that is identified (either via manual or automated monitoring) as unusual, therefore, should not be automatically considered suspicious, but should cause the RFI to conduct further, objective enquiries to determine whether or not the transaction or conduct is indeed suspicious.

VIII.198 Enquiries into unusual transactions should be in the form of additional CDD measures to ensure an adequate, gap-free understanding of the transaction and/or relationship, including the purpose and nature of the transaction and/or conduct and the identity of the persons who initiate or benefit from the transaction and/or conduct.

VIII.199 All employees, regardless of whether they have a formal compliance role, are obliged to report to the Reporting Officer within the RFI each instance in which they have knowledge, suspicion, or reasonable grounds to know or suspect that funds, digital asset or other assets are the proceeds of crime or that a person is involved in money laundering or terrorist financing. RFIs should ensure that they establish and communicate the channels available for all employees to escalate potentially suspicious activity. Additionally, identification and escalation of suspicious activity by employees should be periodically addressed in training, as part of the RFIs employee training programme.

VIII.200 In many circumstances, for purposes of reporting ML/TF suspicion, an agent will be deemed to be an RFI's employee, and therefore must report to the RFI's Reporting Officer. In addition, where an RFI has a suspicion concerning one of its agents, the RFI must also report such suspicions to the Reporting Officer.

VIII.201 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 to know or suspect that funds, digital asset or other assets are the proceeds of crime or that a person is involved in money laundering or terrorist financing.

VIII.202 Where, after evaluating an internal suspicious activity report, the Reporting Officer determines that there is knowledge, suspicion or reasonable grounds to know or suspect that funds, digital assets or other assets are the proceeds of crime or that a person is involved in money laundering or terrorist financing, the Reporting Officer must promptly file an external suspicious activity report with the Financial Intelligence Agency after this knowledge or suspicion comes to his/her attention.

VIII.203 As of October 2011, the Financial Intelligence Agency no longer accepts any manually submitted suspicious activity reports (including those faxed or e-mailed). The Financial Intelligence Agency accepts only those suspicious activity reports that are submitted electronically via the goAML system, which is available at www.fia.bm. The reporting officers of all DABs are required to register with the FIA as soon as practical, so as to be able to be in a state of preparedness to file a report promptly, when the need arises.

VIII.204 Where a Reporting Officer considers that an external report should be made urgently, initial notification to the Financial Intelligence Agency may be made by telephone, but must be promptly followed up by a full suspicious activity report.

VIII.205 The Financial Intelligence Agency is located at 6th Floor, Strata 'G' Building, 30A Church Street, Hamilton HM11 and it can be contacted during office hours on telephone number (441)-292-3422, on fax number (441)-296-3422, or by e-mail at info@fia.bm.

Failure to report and tipping-off offences

VIII.206 Where an employee, including in many circumstances, an agent, fails to comply with the obligations under Section 46 of POCA 1997 or in paragraph 1 of Schedule 1 to ATFA 2004 to make disclosures to a Reporting Officer and/or to the Financial Intelligence Agency promptly after information giving rise to knowledge or suspicion comes to the attention of the employee, the employee or agent is liable to criminal prosecution.

VIII.207 The criminal sanction, under POCA 1997 and ATFA 2004, for failure to report, is a prison term of up to three years on summary conviction or ten years on conviction in indictment, a fine up to an unlimited amount, or both.

VIII.208 Section 47 of POCA 1997 and Section 10A of ATFA 2004 contain tipping-off offences.

- It is a tipping-off offence under Section 47 of POCA 1997 and Section 10A of ATFA 2004 if a person knows or suspects that an internal or external report has been or is being made to the Reporting Officer or to the Financial Intelligence Agency and the person discloses to any other person:
- Knowledge or suspicion that a report has been or is being made; and/or
- Any information or other matter likely to prejudice any investigation that might be conducted following such a disclosure.

VIII.209 It is also a tipping-off offence if a person knows or suspects that a police officer is acting, or proposing to act, in connection with an actual or proposed investigation of money laundering or terrorist financing and the person discloses to any other person any information or other matter likely to prejudice the actual or proposed investigation.

VIII.210 Any approach to the customer or to an introducing intermediary should be made with due regard to the risk of committing a tipping-off offence. See paragraphs 9.83 through 9.84.

VIII.211 Detailed information on suspicious activity reporting, including related offences and constructive trusts is set forth in Chapter 9: Suspicious Activity Reporting of the main guidance notes.

Employee and agent training and awareness

In addition to the training guidelines set forth in Chapter 10 of the main BMA guidance notes, the Authority requires that RFIs with DABs be cognisant of the below information with respect to training employees and agents.

VIII.212 The responsibilities of RFIs to ensure appropriate employee training and awareness are governed primarily by Regulations 16 and 18 of the Bermuda Proceeds of Crime (anti-money laundering and anti-terrorist financing) Regulations 2008.

VIII.213 In many circumstances, an RFI conducing DAB will have one or more agents who, for AML/ATF purposes, are considered employees of the RFI and must be trained as such.

VIII.214 RFIs must take appropriate measures to ensure that relevant employees and agents:

- Are aware of the Acts and Regulations relating to ML/TF;
- Undergo training on how to identify transactions which may be related to ML/TF; and
- Know how to properly report suspicions regarding transactions that may be related to ML/TF.

VIII.215 Each RFI should establish a comprehensive AML/ATF training programme. This programme should address the frequency in which new and existing employees will receive general AML and sanctions training and must also ensure that relevant employees and agents receive appropriate training on its AML/ATF policies and procedures relating to:

- Customer due diligence measures;
- Ongoing monitoring;
- Record-keeping;
- Internal controls; and
- Risk assessment and management.

VIII.216 Where an employee, including in many circumstances, an agent exercises discretion for or in relation to a customer, the RFI must ensure that the employee or agent as the case may be 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. In order to mitigate the risks of an employee exercising discretion, the DAB or RFI should consider documenting guidelines around when discretion can be exercised in appropriate policies and/or procedures.

VIII.217 Detailed information on employee training and awareness is set forth in Chapter 10: Employee Training and Awareness.

Record-keeping

VIII.218 The record-keeping obligations of RFIs are governed primarily by Regulations 15 and 16 of the Bermuda Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008.

VIII.219 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 linked transactions, is completed.

VIII.220 Where an RFI conducting DAB engages in transactions that are eligible for simplified CDD, the RFI must keep records of any CDD performed. Where the RFI has determined on the basis of the Acts and Regulations and its AML/ATF risk assessment that no CDD is required for a particular transaction, the RFI must nonetheless keep records of the transaction itself.

VIII.221 Such records should be of a nature as to permit the reconstruction of individual transactions and include information related to the exchange, conversion, purchase, sale, transfer, or transmission of digital assets specifically as it relates to:

- the identity and physical addresses of the party or parties to the transaction that are customers or account holders, to the extent practicable, any other parties to the transaction;
- the amount or value of the transaction, including in what denomination purchased, sold, or transferred;
- the method of payment;
- the date or dates on which the transaction was initiated and completed; and
- a description of the transaction.

VIII.222 Detailed information on the records that must be kept is set forth in Chapter 11: Record-Keeping of the main guidance notes.

Digital asset businesses as customers of other RFIs

VIII.223 Many DABs are reliant upon access to the regulated financial sector in order to commence or continue their operations. Some financial institutions, perceiving DABs to be high-risk for ML/TF for the reasons set forth in paragraph VIII.53 herein, 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.224 In order to become or remain a customer of another RFI, a DAB may be asked by the other RFI to provide detailed information concerning one or more of the following:

- Whether the business is properly licensed, registered and regulated;
- Whether the business is a principal in its own right, or an agent of another principal;
- Length of time the business has operated;
- Identity, experience and reputation of the business's beneficial owners and managers;
- The business's formal AML/ATF policy statement (see paragraphs 1.29 through 1.35);

- The business's AML/ATF policies, procedures and controls, including group-wide compliance programmes;
- Names and contact information for the business's Compliance Officer and Reporting Officer (see paragraphs 1.36 through 1.49);
- The business's internal and/or independent audits of the functioning of its AML/ATF policies, procedures and controls (see paragraphs 1.75 through 1.79); of the main guidance;
- The business's policies, procedures and controls for screening, onboarding, training and overseeing agents and employees;
- The business's agent list;
- The business's client profile;
- The business's products and services profile;
- Purpose of the proposed account and the type and level of anticipated account activity; and
- The business's assessment of the ML/TF risks it faces, and the mitigating measures it has put in place.

Risk factors for digital asset business

VIII.225 In addition to the non-exhaustive list of risk factors set forth above and in paragraph 2.35 of the main guidance notes, RFIs conducting DAB should consider sector-specific risk factors, including those in paragraphs VIII.57 and VIII.226 to VIII.231, in order to fully assess the ML/TF risks associated with a particular business relationship. The non-exhaustive list of sector-specific risk factors addresses customers, products, services, transactions, delivery channels, agents and other third parties, and geographic connections.

VIII.226 ***Customer risk factors include, but are not limited to:***

- A customer who offers false, fraudulent, or fictitious identification information or documents;
- Unjustified delays in the production of identity documents or other requested information;
- A non-face-to-face customer, where doubt exists about the identity of the customer;
- A customer who knows little or is reluctant to disclose basic details about the payee;
- A customer who has only vague knowledge about the amount of money involved in the transaction;
- A customer who gives inconsistent information;
- A customer transacting with a jurisdiction with which the customer has no apparent ties;
- A customer who appears to be acting on behalf of a third party but does not disclose that information;
- One or more persons other than the customer watching over the customer or waiting just outside of the RFI;
- A customer reading from a note or mobile phone while providing details of the transaction;
- A customer travelling unexplained distances to different locations of the RFI and/or its agents to conduct transactions;

- 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;
- A customer who owns or operates a cash-based business;
- The involvement of any PEPs as a person owning, controlling or representing the customer, or as a person otherwise connected with the customer;
- A customer who is known to the RFI to have been the subject of law enforcement sanctions in relation to crime generating proceeds;
- A customer who begins a transaction, but cancels the transaction after learning of a CDD requirement;
- A customer who threatens or tries to convince the RFI's personnel to avoid reporting;
- A customer who is a member of a class of persons considered higher risk for ML/TF;
- The unnecessary granting of a power of attorney;
- A customer who is unwilling or unable to provide satisfactory information to verify the source of wealth or source of funds;
- Levels of assets or transactions that exceed what a reasonable person would expect of a customer with a similar profile;
- A customer offering to pay extraordinary fees for unusual services, or for services that would not ordinarily warrant such a premium;
- 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;
- Requests for anonymity that go beyond a reasonable request for discretion;
- A customer or counterpart who is another DAB or financial institution which has been sanctioned by a respective national competent authority for non-compliance with applicable AML/ATF regulations and who is not engaging in remediation to improve its compliance;
- A customer who uses agents or associates such that it is difficult for the RFI to identify the beneficial owner of the funds;
- 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;
- A customer that is involved in online gambling; and
- A customer that transacts with mixing/tumbler services or the dark web.

VIII.227 ***Products and services risk factors include, but are not limited to:***

- Products or services that may inherently favour anonymity;
- Products that can readily cross international borders, such as cash, online money transfers, stored value cards, money orders and international money transfers by mobile phone;
- Products or services that have a very high or no transaction limit; and

- Products or services that permit the exchange of cash for a negotiable instrument, such as a stored value card or a money order.

VIII.228 ***Transaction risk factors include, but are not limited to:***

- Transactions that are just below the RFI's thresholds for due diligence checks;
- Transactions that appear to have no obvious economic or financial basis;
- Unusual, complex or uncharacteristically large transactions;
- Transactions that route through third countries or third parties, including mixers;
- Transactions that can be traced to or from the dark web or mixing /tumbler services;
- Transactions accompanied by information that appears false or contradictory;
- A wire transfer or money transmission that is not accompanied by all required information;
- A transaction to a country or region that is outside of the RFI's normal business;
- Large cash or bearer instrument transactions in circumstances where such a transaction would normally be made by cheque, banker's draft or wire transfer;
- Transfers to the same person from different individuals or to different persons from the same individual with no reasonable explanation;
- Transfers of funds that are not in line with the stated business activities of the customer;
- Customers requesting transfers to or from overseas locations with instructions for payment to be made in cash;
- Transactions from another DAB that is not acting as the RFI's agent;
- 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;
- One-off transactions giving rise to suspicion; and
- Requests for funds, shares or other assets to be transferred to PEPs or higher-risk charities or other not-for-profit organisations not subject to effective supervision and monitoring.

VIII.229 ***Delivery channel risk factors include, but are not limited to:***

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

VIII.230 ***Agent and other third party risk factors include, but are not limited to:***

- Agents for which the RFI is unable to satisfactorily complete the steps set forth in paragraph VIII.168;
- Agents that refuse to provide information requested for inclusion in the RFI's agent list;

- Agents representing more than one RFI;
- An agent that has its own agents for which it provides inadequate supervision;
- Agents located in a higher-risk jurisdiction or serving higher-risk customers or transactions;
- Agents that are, or involve, PEPs;
- Agents conducting an unusually high number of transactions with another agent location, particularly with an agent in a high risk geographic area or corridor;
- Agents that have transaction volume that is inconsistent with either overall transaction volume or relative to typical past transaction volume;
- Agents that have been the subject of negative attention from credible media or law enforcement sanctions;
- Agents that have failed to attend or satisfactorily complete the RFI's training programs;
- Agents that do not effectively manage compliance with the RFI's AML/ATF policies, procedures and controls;
- Agents that fail to provide required originator information upon request;
- Agents that conduct inconsistent or substandard data collection or record keeping;
- 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;
- 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;
- 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;
- Agents who move money through RFI accounts in amounts not corresponding with the agent's digital asset business on behalf of the RFI;
- Agents that are new businesses without an established operating history; and
- An agent that fails the RFI's transaction testing for compliance with the RFI's AML/ATF policies, procedures and controls.

VIII.231 ***Geographic risk factors include, but are not limited to:***

- A customer entity established with funds originating from banks in high-risk jurisdictions;
- 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;
- A DAB transaction to, though, or from a high-risk jurisdiction;
- A non-face-to-face transaction initiated from a high-risk jurisdiction;
- A DAB transaction linked to business in or through a high-risk jurisdiction;
- 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

- 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.

***