AML/CFT/CPF GUIDELINES
Date Issued: 1 May 2009
Last Revised: 19 March 2026

CENTRAL BANK OF THE BAHAMAS

GUIDELINES FOR SUPERVISED FINANCIAL INSTITUTIONS ON THE PREVENTION OF MONEY LAUNDERING, COUNTERING THE FINANCING OF TERRORISM & PROLIFERATION FINANCING

Disclaimer: These Guidelines are subject to periodic review and amendment by the Central Bank of The Bahamas

TABLE OF CONTENTS

APPENDICES **PAGES**

SCOPE

The Central Bank of The Bahamas ("the Central Bank") is responsible for the licensing, registration, regulation and supervision of supervised financial institutions ("SFIs") operating in and from within The Bahamas, pursuant to the Banks and Trust Companies Regulation Act, 2020 ("BTCRA"), the Central Bank of The Bahamas Act, 2020 ("CBBA"), and The Bahamas Cooperative Credit Unions Act, 2015 ("BCCUA"), the Payment Systems Oversight (Regulations) 2012, the Payment Services Act, 2012 and any other applicable financial services legislation.

In carrying out its statutory mandate, the Central Bank is designated as the competent authority for ensuring that SFIs establish, implement, and maintain effective systems, policies, procedures, and controls to prevent and detect money laundering (ML), terrorist financing (TF), and proliferation financing (PF). These obligations form an integral part of the Central Bank's prudential and conduct-of-business supervisory framework and are applied in accordance with a risk-based approach.

All SFIs are required to comply with the Central Bank's licensing, registration, prudential and ongoing supervisory requirements, including periodic onsite examinations, thematic reviews, and regulatory reporting. SFIs must also conduct their affairs in full conformity with the AML/CFT/CPF legal and regulatory framework of The Bahamas, inclusive of the Financial Transactions Reporting Act, the Financial Intelligence (Transactions Reporting) Regulations, and any applicable Guidelines, directives, or notices issued by the Central Bank or other competent authorities.

The BTCRA empowers the Inspector of Banks and Trust Companies ("the Inspector") to assess the adequacy and effectiveness of SFI's AML/CFT/CPF frameworks, including customer due diligence (CDD), ongoing monitoring, record keeping, internal controls and governance arrangements. The Inspector is authorised to conduct onsite and offsite supervision to determine SFIs compliance with applicable laws, regulations, and Guidelines, and to take enforcement action where deficiencies are identified.

These Guidelines set out the mandatory minimum requirements of the AML/CFT/CPF laws of The Bahamas and industry best practices and are enforceable by virtue of regulation 8 of the Financial Intelligence (Transactions Reporting) Regulations 2001.

All SFIs must use these Guidelines to develop and implement AML/CFT/CPF frameworks that are proportionate to the nature, size, complexity, and level of risk profile of their business. If a SFI has deviated from these requirements, there may be sanctions under the applicable legislation.[1]

[1] Pursuant to regulation 8 of the Financial Intelligence (Transactions Reporting) Regulations 2001, failure to comply with these Guidelines is an offence that may attract a fine of up to B$50,000.00 for the first offence and up to B$100,00.00 for subsequent offences. See also the section in these Guidelines entitled "Penalties for Non-Compliance".

Money laundering prevention, countering the financing of terrorism and countering proliferation financing should not be viewed as stand-alone compliance functions. SFIs are required to embed AML/CFT/CPF considerations into their ML/TF/PF risk assessment and, where appropriate, incorporate them into their enterprise-wide risk management frameworks, governance structures, and strategic decision-making processes. It is vital that the management team, inclusive of senior management and boards of directors, of every SFI foster a culture of compliance, money laundering prevention, countering the financing of terrorism and proliferation financing as part of their overall risk management strategy and demonstrate intolerance to financial crime as a whole. These obligations go beyond a stand-alone requirement imposed by legislation.

Where a SFI is a part of an international group, it must follow the group policy to the extent that all overseas branches, subsidiaries and associates where control can be exercised, ensure that money laundering prevention and countering the financing of terrorism standards and practices are undertaken at least to the standards required under Bahamian law or, if standards in the host country are considered or deemed more rigorous, to those higher standards. The reporting procedures for suspicious transaction reports ("STRs") under the applicable domestic anti-money laundering and anti-terrorism legislation in The Bahamas must be adhered to.

The Financial Intelligence Unit ("the FIU") issues guidelines[2] in relation to suspicious transaction reporting ("STR"), anti-money laundering policies and procedures, and other reporting obligations under the Financial Transaction Reporting Act, and related regulations. Such guidance focuses primarily on the identification, submission, and handling of STRs and other prescribed reports.

Accordingly, in addition to compliance with these Guidelines issued by the Central Bank, SFIs should also adhere to the FIU's Guidelines on suspicious transactions reporting.

Consistent with the requirements of the law these Guidelines cover:-

- Internal controls, policies and procedures (Section II);
- Risk Rating Customers (Section III);
- Verification of Customer Identity (Section IV);
- Money Transmission Businesses (Section V);
- Electronic Funds Transfers (VI); Record Keeping (Section VII);
- The Role of the Money Laundering Reporting Officer ("MLRO") (Section VIII); and
- Education and Training Requirements (Section IX)

[2] Financial Intelligence Unit, *Suspicious Transaction Report Reporting Guidelines*, published 5 May 2021 (Financial Intelligence Unit of The Bahamas), available at https://www.fiubahamas.org.bs/suspicous-transreport-guide/

In the event of any inconsistency, SFIs must ensure compliance with the requirements of the applicable primary legislation and regulations, applying the higher or more stringent standard where appropriate.

I - BACKGROUND

Bahamian Anti-Money Laundering and Anti-Terrorism Legislative Framework

1 The law of The Bahamas specifically concerning money laundering and terrorist financing is contained in the following legislation[3]:

- the Anti-Terrorism Act, 2018 ("ATA");
- the Financial Transactions Reporting Act, 2018 ("FTRA");
- the Financial Transactions Reporting Regulations, 2018 ("FTRR");
- the Financial Transactions Reporting (Wire Transfers) Regulations, 2018 ("the Wire Transfers Regulations");
- the Financial Intelligence Unit Act, 2023 ("FIUA");
- the Financial Intelligence (Transactions Reporting) Regulations, 2001;
- the Proceeds of Crime Act, 2018 ("POCA")
- the Travellers Currency Declaration Act, 2015; and
- Register of Beneficial Ownership Act, 2018 ("ROBO Act").

2 Developments at the international level, particularly the evolving standards and interpretive guidance issued by the Financial Action Task Force ("FATF"), underscore the importance of a holistic, risk-based approach to anti-money laundering, countering terrorist financing, and countering proliferation financing.

3 Since 2018, concepts such as identified risk and the Identified Risk Framework (IRF) have reflected a deliberate shift toward outcomes focused supervision and risk management, consistent with FATF's emphasis on effectiveness.

4 Therefore, SFIs are expected to ensure that their AML/CFT/CPF frameworks are sufficiently dynamic, forward-looking, and proportionate, and that they are capable of responding to both domestic and international risk developments as articulated by FATF and other relevant standard-setting bodies.

[3] A provision of a statute or regulation is, unless otherwise indicated, deemed to include a reference to such provision as amended, modified or re-enacted from time to time.

5 The abovementioned laws align with international standards and best practices, particularly the FATF standards and its interpretative guidance.

6 Of particular note, the FTRA continues to be robust, and consistently evolving to align with the FATF Standards. Among other things, the FTRA as amended, has placed a requirement upon financial institutions to conduct customer due diligence on a risk-based schedule (see additional guidance under the section "Development a Risk Rating Framework") in line with the FATF Standard.

Penalties for Non-Compliance

7 In addition to these Guidelines, SFIs must comply with the obligations imposed by the Acts listed above and any associated Regulations. Revisions have been effected to the laws which allow for the imposition of criminal prosecution and/or penalties. In addition to fines, offences under the POCA may attract prison terms between seven and twenty years upon summary conviction (see section 15 of the POCA).

8 The offences outlined in Part V of the FTRA attract prison terms of up to five years, fines of $500,000, or both. In that part, the requirements imposed upon financial institutions apply to directors, partners, officers, principals and employees as well. Under the FTRA, the Central Bank is also empowered to impose administrative penalties of up to $200,000 for a company or up to $50,000 for an employee, director or senior manager of a SFI - where these persons contravene the provisions of the FTRA, the POCA or any regulations made under those Acts, including the FTRR and the Wire Transfers Regulations. SFIs are, therefore, reminded to take all necessary steps to ensure full compliance with Bahamian laws (see section 57 of the FTRA and regulation 17 of the Wire Transfers Regulations).

9 Under the ATA, the financing of terrorism is an offence, as is the financing of proliferation of weapons of mass destruction. These offences include the provision of financial services, or the attempt to provide financial services with the intention or knowledge that the funds will be used for certain illicit purposes. These offences attract fines and or/imprisonment for individuals, or directors and persons in charge of legal entities.

What Is Money Laundering?

10 Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the profits (or proceeds) of their criminal acts. If undertaken successfully, it allows them to maintain control over those proceeds and, makes them appear legitimate (see sections 9, 10 and 11 of the POCA).

The Need to Prevent Money Laundering

11 To benefit from the proceeds of their activities, those involved need to exploit the facilities of the world's financial institutions. Thus, the ability to launder the proceeds of criminal activity through the financial system is vital to the success of criminal operations. The increased integration of the world's financial systems, and removal of barriers to the free movement of capital have increased the ease with which proceeds of crime can be laundered, and complicated the tracing process.

12 It is essential to the fight against crime that, whenever possible, individuals be prevented from appearing to legitimize the proceeds of crime by disguising "dirty" funds as "clean" funds.

13 As a leading financial centre, The Bahamas has an important role to play in combating money laundering and other identified risks. SFIs and individuals that knowingly become involved in money laundering risk prosecution, reputational loss, and the loss of their entitlement to operate in (or from within) The Bahamas.

Stages of Money Laundering

14 There are multiple methods of laundering money. Methods range from the purchase and resale of luxury items (e.g. cars or jewellery) to passing money through a complex international web of legitimate businesses and "shell" companies. Initially, however, the proceeds usually take the form of cash, which needs to enter the financial system by some means.

15 Despite the variety of methods employed, the laundering process is accomplished in three stages. Each stage presents an opportunity to alert a financial institution to criminal activity:

(a) *Placement* - the launderer introduces his illegal profits into the financial system.

(b) *Layering* - the launderer separates illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity;

(c) *Integration* - the launderer attempts to legitimize wealth derived from criminal activity. If the layering process has been successful, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

The three basic stages may occur as separate and distinct phases. They may occur simultaneously, or overlap. This often depends on the available laundering mechanisms and the requirements of the criminal organisations.

16 Understanding the various forms of money laundering is key to helping employees identify suspicious transactions. Compliance Officers ("COs") and Money Laundering Reporting Officers ("MLROs") are encouraged to familiarize themselves with the various typologies (or techniques) of money laundering, terrorism financing and proliferation financing. Typologies may be issued by the Central Bank, other domestic Supervisory Authorities, the FIU, or international standard setting bodies such as the FATF.

17 Certain points of vulnerability have been identified in the laundering process which the money launderer finds difficult to avoid and where the activities are, therefore, more susceptible to being recognised, namely:

- entry of cash into the financial system;
- cross-border flows of cash;
- transfers within and from the financial system;
- acquisition of financial assets;
- incorporation of companies; and
- establishment of financial vehicles (e.g. investment funds).

Vulnerability of Financial Institutions to Money Laundering

18 To combat money laundering, it is best to focus on the points in the process where the launderer's activities are more susceptible to recognition. These are largely concentrated in the deposit taking procedures of financial institutions, i.e., the placement stage. However, there are numerous crimes where cash is not involved. Financial institutions should consider the money laundering risks posed by the products and services they offer, and tailor their AML procedures to mitigate these risks.

19 The most common form of money laundering that domestic SFIs will encounter when conducting their mainstream banking business, is when accumulated cash transactions are deposited in the banking system or exchanged for value. Electronic funds transfer systems increase this vulnerability by enabling the cash deposits to be moved rapidly between accounts in different names and different jurisdictions. International SFIs, by contrast, generally do not deal in cash, or do so only in very limited circumstances, so the main money laundering threat will come from electronic or documentary movement of funds that have been converted from currency elsewhere in the world.

20 Financial institutions provide a wide range of services which are vulnerable to being used in the layering and integration stages of money laundering. Mortgage and other loan accounts may also be used as part of this process to create complex layers of transactions. Appendix A of these Guidelines contains important source materials for money laundering typologies.

Vulnerability of Credit Unions to Money Laundering and Terrorist Financing

21.1 Like other financial institutions that take deposits and give credit, Credit Unions conduct business that can be used to disguise the proceeds of crime or finance terrorism. Credit Unions face the risk that a criminal may place funds into that institution, and then legitimize those funds through a series of transactions.

21.2 The typical credit union does not deliver sufficient functionality or flexibility to be the first choice for large scale money launderers and terrorist financiers. For instance, there are laws constraining a credit union's lending activity and the type of loans which may be granted to a person. However, despite the close network of members, and other restrictions in place, credit unions are still susceptible to the risk of money laundering.

21.3 The high levels of cash transactions passing through credit unions may be one area in particular where there is a higher risk of money laundering or terrorist financing. An example of this is 'smurfing', where several small deposits are made into an account, and the amount of each deposit is unremarkable but the aggregate deposit is significant. Another method is the repayment of larger loans over short repayment periods, or in lump sum payments, where the source of funds is unclear.

21.4 Money launderers and terrorist financers may abuse their membership in a Credit Union to commit money laundering and/or to finance terrorism. Credit Unions in The Bahamas are traditionally community-based organizations, which allows them to become more familiar with their members and the financial services they require; but the risk of money laundering and terrorist financing remains. Criminals may also seek to obtain membership in a Credit Union by providing a false identity or using a legitimate member to conduct illicit third-party transactions.

21.5 Credit Unions provide members with an array of financial services which are similar to services offered by banks **with the exception of** currency exchange, the remittance or transferring of cash to foreign jurisdictions, and insurance products. In essence, they provide savings accounts, fixed deposits, cheque cashing, credit cards and mortgages.

21.6 The governance structure of credit unions can also be an area of vulnerability, if board directors who sometimes fulfill operational roles (such as approving high value loans) do not have AML/CFT/CPF backgrounds or adequate AML/CFT/CPF training.

Terrorism, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction

22 The ATA expands the legislative regime related to terrorism, training and support for terrorist groups, and the financing of proliferation of weapons of mass destruction. It also contains provisions which impose mandatory reporting obligations on SFIs and enhances the mechanisms for international co-operation to combat these crimes.

The ATA applies to actions, persons and property both inside and outside The Bahamas. See Part III of the ATA for additional details on terrorism and terrorism related offences.

23 The ATA defines terrorism as any act which is intended to intimidate the public or coerce a government or international organisation to comply with the demands of terrorists and which is intended to cause death or serious bodily harm to a person, serious risk to public health or safety, substantial damage to property, interference with or disruption of essential services or systems; prejudice to national security or disruption of public safety (including emergency services, electronic systems, infrastructure, etc.). See section 14 of the ATA.

23.1 Under section 49 of the ATA as amended, where a SFI knows or has reasonable grounds to suspect that funds maintained on its books belong to an individual, an entity or a legal entity who —

(a) commits terrorist acts or participates in or facilitates the commission of terrorist acts or the financing of terrorism;

(b) commits acts of proliferation or participates in or facilitates the commission of proliferation acts or the financing of proliferation or

(c) is a designated or a listed entity, the SFI must report the existence of such funds to the FIU.

Likewise, where a SFI knows, or has reasonable grounds to suspect, that funds are linked/related to, or to be used:

- for terrorism;
- for terrorist acts;

- by terrorist organisations; or
- by those who finance terrorism

the SFI must file a suspicious transaction report with the FIU.

23.2 The ATA also criminalises the act of financing of proliferation of weapons of mass destruction ("proliferation financing"). Under section 9 of the ATA, proliferation financing occurs where any person, provides or makes available Funds or financial services, whether directly or indirectly, to persons with the intention or knowledge that such funds are to be used in whole or in part for, amongst other things, the manufacturing, development, production, distribution or supply of nuclear, chemical or biological weapons for use in terrorist acts. It also includes the use of funds or financial services to train persons to develop or produce such weapons for use by terrorists and terrorist organizations. Where a SFI or its director or management is convicted of an offence under section 9, the Court may for example, revoke its licence or order that the SFI be wound up and its assets forfeited.

23.3 Part IV of the ATA contains provisions for implementing the United Nations Security Council Resolutions ("UNSCRs") in The Bahamas, including procedures all SFIs must follow. Specifically, a UNSCR may impose financial sanctions, among other things, on designated individuals and entities that are engaged in, or provide support for, activities and programmes related to terrorism, terrorist groups, and the proliferation of weapons of mass destruction.

23.4 If an individual or entity is designated as a terrorist entity by the UN Security Council, and a SFI receives the list of designated entities from the National Identified Risk Framework Coordinator, the SFI must without delay:

- freeze all of the funds it holds in the name of a designated entity;
- inform the Attorney-General and FIU that it holds the funds of a designated entity and provide details; and
- inform the designated entity that any funds held have been frozen.

The designated entity can commence proceedings in the Supreme Court for an order releasing the frozen funds within 14 days after the date the designated entity was informed about the frozen funds (see section 44 of the ATA).

23.5 Under section 45 of the ATA, after an investigation by the Commissioner of Police, the Attorney-General may apply to a judge for an order declaring that an individual, designated or legal entity is a "listed entity" for the Act's purposes and freezing the property of the listed entity. This triggers a series of obligations. For example, subject to some other factors, the order may prohibit the listed entity from possessing or controlling cash greater than an amount determined by

the judge. The order may also indicate which account in a SFI any excess cash should be placed and restrict access to such funds.

23.6 SFIs are also under a duty to disclose to the FIU forthwith, the existence of any property in their possession or control, which they know or have reasonable grounds to believe is terrorist property or property to which a section 45 order applies. SFIs are also to disclose to the FIU any information regarding a transaction or proposed transaction which they know or have reasonable grounds to believe may involve terrorist property or property to which an order made under section 45 applies (see section 70 of the ATA).

No civil or criminal liability will lie against any person who makes such disclosures or reports in good faith. However, persons who fail to comply with subsections (1) or (3) of section 70 commits an offence and shall be convicted on indictment and liable to imprisonment for five years.

23.7 For further guidance and reference materials, SFIs should refer to Appendix C of these Guidelines, the Central Bank's *"Guidance Notes for Sanctions Screening"* issued 20th November, 2025 and the Group of Financial Services Regulators *"Countering Proliferation Financing Guidelines: For Financial Institutions and Designated Non-Financial Businesses and Professions"* issued on 25th July, 2025.[4]

Tipping Off

24 Under section 30 of the FTRA, a person commits a tipping off offence if he knows or suspects that any disclosure relating to a suspicious transaction has been made, and he makes a disclosure relating to the suspicious transaction which is likely to prejudice any subsequent investigation which might be conducted. More simply, it is an offence to "tip off" (or inform) someone suspected of a financial crime that a suspicious transaction report has been filed, or provide them with other information that might compromise a future investigation.

Preliminary enquiries to verify customer identity and learn the source of funds or precise nature of the transaction being undertaken will not trigger a tipping off offence before an STR has been submitted in respect of that customer unless the enquirer knows that an investigation is underway, or that the enquiries are likely to prejudice an investigation. However, where a SFI forms a suspicion that a transaction relates to an identified risk, and reasonably believes that performing any of the CDD measures will tip-off a customer, or potential

[4] Central Bank of The Bahamas. (2026). *AML/CFT/CPF guidelines and guidance notes for supervised financial institutions*. https://www.centralbankbahamas.com/bank-supervision/aml-cft-cpf-sfi-guidance-notes

customer, the SFI is permitted not to perform those measures. In such cases, SFIs are required to document the basis for their assessment and file an STR.

Where it is known or suspected that an STR has already been filed with the FIU, the Police or other authorised agency, and further enquiries become necessary, SFIs should take great care to ensure that customers remain unaware that their names have been shared with the authorities.

Where any information is disclosed or supplied by any person in a STR, no civil, criminal or disciplinary proceedings shall lie against that person for the disclosure or supply of that information; or for any consequences that follow from the disclosure or supply of that information unless the information was disclosed or supplied in bad faith (see section 28 of the FTRA).

Interpretation

25 In these Guidelines, the following terms shall have these meanings, unless the context otherwise requires:

(a) "AML/CFT/CPF" means anti-money laundering, countering the financing of terrorism and countering the financing of proliferation;

(b) "beneficial owner**"** refers to - a natural person who ultimately owns or controls a facility holder; or is the natural person on whose behalf a transaction or activity is being conducted; or a natural person who exercises ultimate effective control over a legal person or legal arrangement. A beneficial owner may exercise ultimate effective control directly or indirectly, including through ownership chains, joint control, trusted or nominee arrangements, or other forms of power that enable the person to determine, or substantially influence, the entity's actions and decisions. Where no natural person fits squarely into those categories, it is the person who holds the position of senior managing official;

(c) -"CDD" means customer due diligence;

(d) "controlling interest" means direct or indirect shareholders acting individually or as a group holding ten percent or more of the voting rights and shares in an entity;

(e) "Executive Entity" means a legal person established by a Charter to perform only executive functions, registered in accordance with the Executive Entities Act, 2011 which is resident and domiciled in The Bahamas and is able to sue and be sued in its own name;

(f) "facility" means any account or arrangement provided by a financial institution to a facility holder which may be used by the facility holder

to conduct two or more transactions. It specifically includes provision for facilities for safe custody, including safety deposit boxes;

(g) "facility holder" refers to a person in whose name the facility is established and includes-

- any person to whom the facility is assigned;
- where the facility is established in the name of a mere nominee, the ultimate natural person who is the beneficial owner, settlor or beneficiary; and
- any person who is authorised to conduct transactions through the facility.

A person becomes a facility holder when that person is first able to use the facility to conduct transactions.

(h) "financial institution" is defined in Appendix E;

(i) "foreign financial institution" means a financial institution in a foreign jurisdiction that is subject to an equivalent regime of monitoring, supervision and regulation as is herein provided and is subject to equivalent or higher anti-money laundering and anti-terrorism financing standards of regulation as provided for by Bahamian law;

(j) "identified risk" means corruption, cybercrime, human trafficking, money laundering, or financing of proliferation of weapons of mass destruction, terrorism or financing of terrorism or such other risk as the Minister may prescribe by regulations;

(k) "identified risk framework" or "IRF" means the measures or policies designed to minimize or eliminate identified risks;

(l) "Identified Risk Framework Steering Committee" or "IRF Steering Committee" means the committee established under section 6 of the POCA;

(m)"member" means a member of a cooperative credit union;

(n) "Minister" means the Minister of Finance;

(o) "nominee" means a person who holds shares in their name on behalf of another person under any express or implied agreement or arrangement;

(p) "nominee director" means a person who is appointed as a director on behalf of another person under any form of control, instruction, or influence, whether formal or informal, direct or indirect, other than the exercise of proper corporate governance or fiduciary duty;

(q) "occasional transaction" means a one-off transaction or linked transactions, that are carried out by a person otherwise than through a facility in respect of which that person is a facility holder;

(r) "senior management" means an officer or employee of a SFI with sufficient knowledge and seniority to make decisions affecting the SFI's risk exposure which need not involve a member of the board of directors and includes a person responsible for compliance or who is authorised to bind the SFI;

(s) "source of funds" means

(i) the transaction or business from which funds have been generated; and
(ii) the means by which a customer intends to transfer those funds/assets to a facility;

(t) "source of wealth" refers to the means by which a customer acquires his wealth (e.g. through a business or an inheritance);

(u) "supervised financial institution" or "SFI" includes banks, trust companies, credit unions, non-bank money transmission businesses, and any other entity carrying on a business regulated by the Central Bank of The Bahamas;

(v) "ultimate effective control" refers to the person or persons who ultimately exercise control, influence, or decision-making power over a legal entity or legal arrangement, even if they are not the registered owner, operator, or direct holder of rights. Ultimate effective control may be exercised directly or through a chain of ownership, control links, or other arrangements (e.g., rights, agreements, or economic benefits) that enable the holder or group to determine, or substantially influence, the entity's actions and business activities; and

(w) "Trust Corporate Service Provider" or "TCSP" refers to those who undertake any one or more of the following activities, by way of business:

i. acting as a Corporate or Partnership formation Agent;

ii. acting as (or arranging for another person to act as) a Director,

Secretary or Official of a Company or a Partner of a Partnership or as a Foundation Official;

iii. providing administration or management of a Trust, Company, Partnership, Foundation, or for any other legal person or legal arrangement;

iv. providing registered office, business address for accommodation, correspondence for administrative address for a Company, Partnership, Foundation or for any other person;

v. acting as a Resident Agent for the purposes of meeting requirements to hold beneficial ownership or interest information;

vi. acting as (or arranging for another person to act as) a Trustee of a Trust;

vii. acting as (or arranging for another person to act as) a Nominee Shareholder for another legal person; or

viii. acting as a Protector or an Enforcer of a Trust.

It should be noted that under the POCA, a "document" is a record of information kept in any form, including electronic format. Similarly, a "record" is any material on which information is recorded or marked, and which is capable of being read or understood by a person, electronic system or other device. All references to "documents", "documentation", and "records" in these Guidelines are equally flexible. If in doubt about whether a document or record should be accepted or stored in a paper or electronic format, SFIs should contact the Central Bank.

In these Guidelines the terms "money laundering" (ML), "financing of terrorism" and "terrorist financing" (FT/TF) and proliferation financing (PF) include any identified risk activity under the POCA. the ATA, 2018, and the FTRA Act, 2018.

The terms "AML/CFT/CPF" and "identified risks" are, where the context permits, used throughout these Guidelines to refer to the overarching frameworks and obligations for managing the risks of money laundering, terrorist financing, and proliferation financing.

The person whose identity must be verified is described throughout these Guidelines as a "facility holder", which includes a "customer," "client", or "member". The terms will vary and are used interchangeably.

Any other terms used in these Guidelines that are not defined here may be found in the relevant legislation.

Responsibilities of the Central Bank of The Bahamas

26 Deposit-taking institutions are particularly vulnerable to use by money launderers and terrorists. Therefore, the Central Bank maintains a keen interest in measures aimed at countering money laundering, terrorist financing, and other identified risks.

27 These Guidelines will be used as part of the criteria against which the Central Bank will assess the adequacy of a SFI's systems to prevent money laundering and counter terrorist financing. Failure to implement or maintain adequate policies and procedures relating to money laundering and terrorist financing may prevent a SFI from satisfying the criteria for initial or continued licensure in the BTCRA.

28 The POCA requires any person to report any information they obtain which in their opinion indicates that any person has or may have been engaged in money laundering, terrorist financing or proliferation of weapons of mass destruction and to disclose that information to the FIU or the law enforcement authorities.

29 SFIs should also note that in the event of a lawful request for information, in the furtherance of money laundering, terrorist financing or proliferation financing investigations, the Central Bank may provide assistance to other regulatory authorities in The Bahamas as well as overseas regulatory authorities through information exchange as provided for under the CBBA and the BTCRA.

II - INTERNAL CONTROLS, POLICIES AND PROCEDURES

30 SFIs must establish clear responsibilities and accountabilities to ensure that policies, procedures, and controls which deter criminals from using their facilities for money laundering or the financing of terrorism, are implemented and maintained, thus ensuring that they comply with their obligations under the law and under these Guidelines.

Risk Self- Assessments

31 SFIs must assess the risk of money laundering and terrorist financing (ML/TF) and other identified risks they may face in the course of conducting their business. This self-assessment must be conducted and documented to allow SFIs to determine their overall level of vulnerability to identified risks.

32 SFIs should consider using the following steps to assess the level of identified risk that the business may face:

1. Identify and assess inherent risks by adopting a comprehensive risk-based approach.
2. Establish risk tolerance levels from an entity specific, sectoral and relationship level perspective.
3. Establish risk mitigation measures by employing proper controls.
4. Evaluate residual risks by employing a three lines of defense regime.
5. Monitor and review risks by utilizing a proper governance regime.

The process outlined below is a guide to assist SFIs in assessing their level of identified risk.

A SFI may choose the method of risk assessment that best suits its business, as long as the SFI complies with its obligations under applicable laws or regulations. However, risk assessments should be commensurate to the nature, size and complexity of a SFI's business. For example, large financial institutions are likely to have their own systems and methodology for conducting a risk assessment.

Additionally, each SFI should ensure that it has sufficient capacity and expertise to manage the risks it faces. As risks and understandings of risk evolve, a SFI's capacity, mitigating controls and expertise should also evolve proportionally.

33 Risk Assessment Process

Note: The risk assessment framework was initially issued in 2018. Subsequent ML/TF/PF Guidance Notes published in June 2023[5] provide more granular instructions for SFIs, including considerations for proliferation financing, enhanced scenario analysis, and updated national and international risk factors.

33.1 Identify and assess inherent risk

Inherent risk relates to the level of risk a SFI faces before it is mitigated by controls. SFIs should consider all relevant information when identifying and assessing inherent risk. SFIs should consider how the various aspects of their business may be targeted to launder money and finance terrorism or facilitate proliferation financing for example.
At minimum, this analysis must identify and assess the SFI's risks based on the following criteria:

- the types of customers;
- the countries or jurisdictions its customers are from (or located); the countries or jurisdictions where the SFI has operations;
- the SFI's products, services, and delivery channels.

[5] Central Bank of The Bahamas, *ML/TF/PF Risk Assessment Guidance Notes*, June 2023, https://www.centralbankbahamas.com/viewPDF/documents/2023-08-25-18-03-33-MLTFPF-Risk-Assessment-Guidance-Notes-June-2023-Header-Update.pdf

The SFI should also take into account variables such as the purpose of the business relationship, the level of customer assets, volume of transactions and the regularity or duration of the business relationship. This relationship-specific risk assessment should be replicable by any appropriate third party.

Further, SFIs should take into account the threats and vulnerabilities that have been identified through any national risk assessment ("NRA"). Specifically, SFIs should consider vulnerabilities identified in The Bahamas's NRA as well as applicable NRAs of jurisdictions in which the SFI has subsidiaries or customers and sectoral risk assessments on ML/TF/PF. SFIs should assess how these (and any other aspects of their business) make their business vulnerable to identified risks.

SFIs should then assess the probability or likelihood that these aspects of their business could result in ML/TF/PF. The end result of this step will be a likelihood rating for each of the risk areas of your business. For example, a SFI may rate each area from a range of high (highly likely) to low (unlikely) to be used for ML/TF.

33.2 Establish risk tolerance

Risk tolerance is the level of risk that a SFI is willing to accept, and impacts decisions about the risk mitigation measures.

Each SFI should consider:

(i) the risks it is willing and unwilling to accept,
(ii) risks that should be escalated to senior management for a decision, and
(iii) whether the SFI has sufficient capacity and expertise to effectively manage the risks it has or is willing to accept.

33.3 Establish risk mitigation measures

Where the level of risk is within a SFI's risk tolerance, it must ensure that the risk mitigation measures applied are commensurate with the level of risk. Where higher risks are identified, SFIs must take enhanced measures to manage and mitigate those higher risks. Each SFI must document its internal controls and related policies and procedures put in place to mitigate and manage the risks identified by the Central Bank, the SFIs themselves or through any risk assessment carried out at a national level. These policies and procedures must be approved by senior management.

Some risk mitigation measures include:

- determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers, products or a combination of both;
- setting transaction limits for higher-risk customers or products;
- determining the circumstances under which they may refuse to take on or terminate~~/cease~~ high risk customers/products or services;
- determining the circumstances requiring senior management approval (e.g. high risk or large transactions, when establishing relationship with high-risk customers such as PEPs).

33.4 **Evaluate residual risk**

Residual risk is the level of risk remaining after the application of risk mitigation measures. Where the level of residual risk exceeds an SFI's risk tolerance, or where its mitigation measures do not adequately address high risks, the strength of mitigation measures should be increased.

33.5 **Monitor and review risks**

The risk assessment should be kept up-to-date through periodic reviews and when risk factors change. These risk assessments must be made available to the Central Bank annually, or more frequently upon request by the Central Bank. SFIs are also required to monitor, compliance with internal policies, procedures, and controls, and enhance them if necessary. Where appropriate, having regard to the size and nature of their business, SFIs must engage an independent audit function to test the internal AML/CFT/CPF policies, controls and procedures.

New Products, Practices and Technological Developments

34 SFIs must take such measures as may be needed to identify and assess the identified risks that may arise in relation to –

(a) the development of new products and new business practices, including new delivery mechanisms; and

(b) the use of new and developing technologies for both new and pre-existing products.

35 SFIs must undertake the risk assessment prior to the launch or use of such products, practices and technologies, and should take appropriate measures, which are commensurate with the identified risks, to manage and mitigate those risks (see section 5 of FTRA).

36 SFIs offering internet-based and/or telephone products and services should ensure that they have reliable and secure methods to verify the identity of their customers. The level of verification used should be appropriate to the risks

associated with the particular product or service. SFIs should conduct a risk assessment to identify the types and levels of risk associated with their telephone and internet banking applications and, wherever appropriate, they should implement multi-factor verification measures, layered security, or other controls reasonably calculated to mitigate those risks.

37 For the purposes of paragraph 36 above, internet-based and/or telephone products and services include the provision of virtual assets and related virtual asset services offered by SFIs.

38 SFIs offering virtual assets and virtual asset services should refer to the Central Bank's *Digital Asset Guidelines*[6], issued on 12th December 2023, for further guidance on the specific risks posed by virtual assets.

39 Designation of Compliance Officers and the MLRO

39.1 All SFIs are required to establish a point of contact with the FIU to handle the reported suspicions of their staff regarding money laundering or terrorist financing. SFIs are required to appoint an MLRO to undertake this role, and this officer is required to be registered with the FIU. SFIs are also required to appoint a Compliance Officer ("CO") at a senior management level to be responsible for the implementation of and on-going maintenance of the SFI's internal policies, procedures and controls in relation to identified risks. The Central Bank also engages regularly with the MLRO.

39.2 All SFIs are required to:

(i) have in place appropriate procedures, controls and monitoring systems for timely detection and prompt investigation of suspicious activity and if appropriate, subsequent reporting to the FIU;

(ii) ensure that the MLRO, the CO, and any other persons appointed to assist them, have unrestricted and timely access to systems, customer records and all other relevant information necessary to discharge their duties;

(iii) establish close co-operation and liaise with the Central Bank;

(iv) notify the Central Bank of the name(s) of the MLRO and the CO;

(v) include in the notification a statement that the MLRO and the CO are fit and proper persons; and

[6] Central Bank of The Bahamas, Digital Asset Guidelines, 12 December 2023, https://www.centralbankbahamas.com/viewPDF/documents/2023-12-12-10-15-24-Digital-Assets-Guidelines-2023.pdf

(vi) notify the Central Bank where there are any changes to the MLRO and the CO.

39.3 A SFI may choose to combine the functions of the CO and the MLRO depending upon the scale and nature of its business.

39.4 The MLRO must have direct access to the SFI's board and any relevant committees of the board. The MLRO's management reporting line must be independent, to the extent feasible, of executives with profit and loss responsibility.

39.5 SFIs must not restrict COs and MLROs in any way, from communicating with the SFI's board, auditors, or any regulator, either while serving as CO or MLRO, or subsequently.

Hiring Employees

40 SFIs must also establish and implement appropriate policies and procedures to ensure high standards are being followed when hiring employees. To this end, SFIs must deploy screening procedures which effect diligent and appropriate enquiries about the personal history and probity of the potential employee, and obtaining the appropriate references.

41 Internal controls in a group of entities

41.1 For the purposes of paragraphs 41.2 to 41.6, a reference to SFI means a SFI incorporated in The Bahamas.

41.2 SFIs with a branch or subsidiary in a host country or jurisdiction must develop an AML/CFT/CPF group policy that complies with the requirements of The Bahamas's AML/CFT/CPF legislation and these Guidelines, and which is applicable and appropriate to such branch or subsidiary.

41.3 A SFI must develop and implement group policies and procedures for its branches and subsidiaries within the financial group to share information required for the purposes of CDD, and for the management of identified risks. This is subject to the SFI's implementation of adequate safeguards to protect the confidentiality and use of any information shared, and to the extent permitted by the laws of the countries or jurisdictions where its branches and subsidiaries are located.

41.4 Such policies and procedures must include the provision to any compliance officer who conducts group-level compliance, audit, anti-money laundering and counter terrorism financing functions, of the account and transaction

information of facility holders from branches and subsidiaries as necessary to fulfil their functions.

41.5 Where the AML/CFT/CPF requirements in the host country or jurisdiction differ from those in The Bahamas, SFIs must require that the overseas branch or subsidiary apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits.

41.6 Where the law of the host country or jurisdiction conflicts with the laws of The Bahamas such that the overseas branch or subsidiary is unable to fully observe the higher standard, the SFI must apply appropriate additional measures to manage any identified risks, report this to the Central Bank, and comply with such further directions as may be given by the Central Bank.

III - RISK RATING CUSTOMERS

International Standards

42 The Financial Action Task Force ("FATF"), in its International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation[7] (the FATF Standards), recommends that financial institutions adopt a risk-based approach to customer due diligence.

43 In its Guidelines entitled "*Sound management of risks related to money laundering and financing of terrorism*", the Basel Committee on Banking Supervision, supports the adoption and effective implementation of the FATF Standards. The Committee recommends that all banks should be required to "have adequate policies, procedures and controls, including robust customer due diligence (CDD) measures to promote high ethical and professional standards in the banking sector and to prevent the bank from being used, intentionally or unintentionally, for criminal activities".[8] It recognises that "adequate policies and processes" in this context requires the implementation of other measures in addition to effective CDD rules. These measures should also be proportional and risk-based, informed by banks' own risk assessment of ML/FT/PF risks[9].

[7] Financial Action Task Force (FATF), International Standards on Combating Money Laundering, the Financing of Terrorism and Proliferation (Consolidated Version, October 2023), available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

[8] Basel Committee on Banking Supervision (BCBS), *Sound management of risks related to money laundering and financing of terrorism* (revised June 2020), Bank for International Settlements, available at: https://www.bis.org/bcbs/publ/d505.pdf.

[9] Basel Committee on Banking Supervision (BCBS), Core Principles for Effective Banking Supervision, April 2024, Bank for International Settlements, available at: https://www.bis.org/bcbs/publ/d573.htm

44 The FTRA and FTRR, adopt the risk- based approach recommended by the Basel Committee and the FATF. The FTRR gives financial institutions the discretion to determine the appropriate level of information and documentation required to verify customer identity based on the nature and degree of risk inherent in the customer relationship.

Developing a Risk Rating Framework

45 Every SFI is required to develop and implement a risk rating framework which is approved by its Board of Directors as being appropriate for the type of products offered by the SFI, and capable of assessing the level of potential risk each client relationship poses to the SFI. As part of the on-going onsite examination program, Central Bank onsite examiners will assess the adequacy of SFI's risk rating policies, processes and procedures, in light of the risks that have been identified by the SFI or notified to it by the Central Bank, as well as the extent to which SFIs have adhered to legislative requirements.

46 As a minimum the risk rating framework relating to client relationships should include:

- differentiation of client relationships by risk categories (such as high, moderate or low);

- differentiation of client relationships by risk factors (such as products, client type/profession, country of domicile, complexity of ownership and legal structure, source of business, type of assets, size and volume of transactions, type of transactions, cash transactions, adherence to client activity profile);

- the KYC documentation and due diligence information requirements appropriate for each Risk Category and Risk Factor based on a prior risk analysis; and

- a process for the approval of the downgrading/upgrading of risk ratings through the periodic review of the customer relationship.

47 SFIs shall review high-risk customers more frequently than other customers. Senior management shall determine the measures required to manage and mitigate heightened risks. Where such risks cannot be adequately managed or mitigated, senior management shall determine whether the customer relationship is to be continued or terminated. All decisions relating to high-risk relationships, including the rationale for such decisions, should be properly documented.

48 Pursuant to section 7A of the FTRA 2025, as amended, and having regard to its risk rating framework, a SFI is required to conduct customer due diligence at a minimum frequency of:

- Annually for high-risk accounts;
- Every three to five years for medium risk accounts; and
- Every five to ten years for low-risk accounts.

Notwithstanding the foregoing, where the SFI identifies or suspects any activity related to an identified risk under the POCA, the SFI shall immediately undertake enhanced due diligence in accordance with these Guidelines.

49 In determining the risk profile of any customer, SFIs should take into account factors such as the following risk criteria. They are not set out in any particular order, nor should they be considered exhaustive:

(i) geographical origin of the customer;

(ii) geographical sphere of the customer's business activities including the location of the counterparties with which the customer conducts transactions and does business, and whether the customer is otherwise connected with certain high-risk jurisdictions, or those known to the SFI to lack proper standards in the prevention of money laundering, countering the financing of terrorism or in the customer due diligence process;

(iii) nature of the customer's business, which may be particularly susceptible to money laundering or terrorist financing risk, such as casinos or other businesses that handle large amounts of cash;

(iv) nature of activity;

(v) frequency of activity;

(vi) customer type (e.g. potentates/politically exposed persons ("PEPs"));

(vii) type, value and complexity of the facility;

(viii) unwillingness of the customer to cooperate with the SFI's customer due diligence process for no apparent reason;

(ix) pattern of account activity given the SFI's information on the customer;

(x) for a corporate customer, an unduly complex ownership structure for no apparent reason;

(xi) whether there is any form of delegated authority in place (e.g. power of attorney);

(xii) the product or service used by the customer (e.g. bearer shares);

(xiii) situations where the origin of wealth and/or source of funds cannot be easily verified or where the audit trail has been deliberately broken and/or unnecessarily layered;

(xiv) whether an account/business relationship is dormant; and

(xv) any other information that raises suspicion of the customer being connected to money laundering or terrorist financing.

50 Prospective Customers

SFIs must assess the potential risk inherent in each new client relationship prior to establishing a business relationship by conducting a risk assessment in accordance with the guidance provided in these Guidelines (see Parts II and III). This assessment should take account of whether and to what extent a customer may expose the SFI to money laundering, terrorist financing or proliferation financing risks by assessing *inter alia*, the nature of the customer, the product or facility to be used by the customer, and any jurisdictional risks. Based on the outcome of this assessment, the SFI should decide whether or not to establish a relationship or provide the requested facility for the customer concerned, in accordance with sections 5(2) and 7(3) of the FTRA.

IV - VERIFICATION OF CUSTOMER IDENTITY

51 For the purposes of these Guidelines, "identity" means the unique set of attributes which define a natural or legal person. There are two main constituents of a person's identity -:

(a) the physical identity (e.g. name, date of birth, registration number); and

(b) the activity undertaken**.**

What is required

52 Supervised Financial Institutions ("SFIs") are required to conduct customer due diligence ("CDD") measures when establishing a business relationship, opening an account, or maintaining an existing account or facility for a customer or facility holder.

SFIs must not establish, maintain, or operate anonymous accounts or accounts in fictitious names, and must not permit the use of pseudonyms, numbered accounts, or any other naming conventions that obscure, conceal, or otherwise

prevent the immediate identification of the true identity of the customer or beneficial owner.

SFIs must ensure that all accounts and business relationships are established and maintained in a manner that promotes transparency and enables the clear identification and verification of the customer and beneficial owner. Account structures, naming conventions, or other arrangements must not be used in a manner that conceals the identity of the customer or beneficial owner or otherwise undermines transparency.

To comply with these obligations, every SFI must:

a) identify and verify the identity of the customer or facility holder using reliable, independent source documents, data, or information;
b) identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, such that the SFI is satisfied that it knows who the beneficial owner is;
c) understand and document the ownership and control structure of any legal person or legal arrangement that is a customer, commensurate with the level of risk;
d) identify and verify the identity of any person purporting to act on behalf of the customer, and verify that such person is properly authorized to act in that capacity; and
e) maintain accurate, adequate, and up-to-date records relating to the identity of the customer and beneficial owner.

SFIs must also review existing accounts and relationships to ensure that no anonymous, fictitious, pseudonymous, or otherwise opaque account arrangements remain in operation. Where the SFI is unable to obtain or verify the information necessary to identify the customer or beneficial owner, the SFI must apply appropriate remedial measures, which may include restrictions on the account, remediation of the deficiency, or termination of the business relationship in accordance with applicable laws and regulatory requirements, and paragraph 56 of these Guidelines.

Nature and Scope of Activity

53 When commencing a business relationship, SFIs should record the purpose and reason for establishing the business relationship, and the anticipated level and nature of activity to be undertaken. The extent of documentary evidence will depend on the nature of the product or service. Documentation about the nature of the applicant's business should also cover the origin (or source) of funds to be used during the relationship.

54 When considering entering into a business relationship, certain principles should be followed when ascertaining the level of identification and verification

checks to be completed. See Appendix D for a flow chart summary of the different steps involved.

55 Reasonable measures should be taken to obtain sufficient information to distinguish those cases in which a business relationship is commenced or a transaction is conducted with a person acting on behalf of others.

Where CDD Measures are Not Completed

56 If a SFI is unable to comply with relevant CDD requirements or in circumstances in which the SFI is not satisfied that the transaction for which it is or may be involved is bona fide, the SFI:

(i) must not open the account or establish the business relationship;

(ii) must not carry out the transaction;

(iii) must terminate the business relationship; and

(iv) consider filing a suspicious transaction report with the FIU.

Any SFI that intentionally opens an account, establishes a business relationship, carries out a transaction, or fails to terminate a business relationship without fulfilling the requirements of sections 5 - 9 and 14 of the FTRA commits an offence, and will be liable upon summary conviction to a fine of up to five hundred thousand dollars, imprisonment for two years, or both. Legal persons may be liable to a fine of up to one million dollars. See section 11 of the FTRA.

57 Once a business relationship has been established, reasonable steps should be taken by the SFI to ensure that descriptive due diligence information is accurate and kept up to date through periodic reviews of existing records. SFIs should refer to paragraphs 74 - 77 of these guidelines for guidance on when further verification of a customer's identity may be necessary.

58 In circumstances where the SFI opts to discontinue the relationship, funds held to the order of the prospective client should be returned only to the source from which they came, and not to a third party unless otherwise directed by a court order.

TIMING FOR VERIFICATION

59 Subject to paragraph 24, SFIs must observe the following timeframes when seeking to verify the identity of their customers:

(a) in the case of prospective customers, SFIs must verify customer identity before permitting them to become facility holders;

(b) in the case of persons who conduct occasional transactions, SFIs must verify identity before the transaction is conducted;

(c) if it appears to a SFI that the person conducting the transaction is doing so on behalf of any other person or persons, the identities of the third parties must be verified before the transaction is conducted;

(d) if there is a suspicion of activities relating to identified risks involving the facility holder or the facility holder's account verification measures must be completed before the facility holder may conduct any further business; and

(e) if during the course of the business relationship the SFI has reason to doubt the identity of the customer, verification measures must be completed before the facility holder may conduct any further business.

60 Existing Customers

SFIs should review the KYC documentation for their existing customers to ensure compliance with the FTRA, the FTRR, the ATA, any other applicable laws of The Bahamas, and the SFI's internal KYC requirements. SFIs must perform CDD measures in relation to existing customers on the basis of materiality and risk and at appropriate times, taking into account any previous measures applied and when the measures were last applied and the adequacy of the information and data obtained.

IDENTIFICATION PROCEDURES

A. Natural Persons

61 When seeking to verify the identity of natural persons, SFIs are to follow the guidance set out in the following paragraphs of this section A. In addition, SFIs must adhere to the streamlined requirements for account opening, provision of financial services and customer identification for natural persons set out in Appendix B.

A SFI must obtain and document the following information when seeking to verify identity:

(i) full and correct name/names used;

(ii) two or more means of contacting the customer (see Appendix B);

(iii) date and place of birth;

(iv) purpose of the account; and

(v) the nature of the business relationship.

62 In addition, the following information may also be obtained and documented:

(i) nationality;

(ii) occupation and name of employer (if self-employed the nature of the self-employment);

(iii) estimated level of account activity including:

(a) size in the case of investment and custody accounts;

(b) balance ranges, in the case of current and deposit accounts;

(c) an indication of the expected transaction volume of the account;

(iv) source of funds;

(v) a specimen signature;

(vi) telephone and fax number, if any; and

(vii) a copy of one or more of the identification documents described in Appendix B.

63 In circumstances where the SFIs' customer is considered a high-risk client, the SFI should also confirm the customer's source of wealth.

A1. Confirmation of Mailing Address, Residential Address and Other Points of Contact

64 SFIs must now maintain at least two (i.e. two or more) current means of contacting each customer who is a natural person. SFIs should verify one or more points of contact from the list in Step 2 of Appendix B. This is consistent with the FTRR which requires that financial institutions obtain contact information when verifying their customer's identity (see regulation 4(1)(b)).

65 SFIs must develop flexible internal procedures when verifying the accuracy of contact information provided. SFIs must obtain independent verification of the residential address (and where relevant, the business address) of customers resident in countries where such verification is reasonably achievable. As a rule of thumb, verification is "reasonably achievable" in every country offering regular delivery of mail to individual homes and businesses. Where this is not the case, or where mail delivery is sporadic, SFIs may rely on more immediate and reliable points of contact. This provides a more efficient and predictable means of managing the risk of fraud, money laundering, and other identified risks.

66 SFIs may use a variety of sources to verify mailing address, *including but not limited to*:

- a letter from a suitable referee (see Appendix B)
- the Register of Electors;
- a tax assessment, bank or credit union statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined);
- a letter from the Department of Social Services or a similar organisation (where the individual is not financially responsible for their accommodations, or otherwise lacks documentary evidence of their address);
- the telephone directory; or a home visit.

67 Where a proposed facility holder's address is temporary accommodation, such as, for example, an expatriate on a short-term overseas contract, SFIs should adopt flexible procedures to obtain verification under other categories, such as a copy of a contract of employment, or banker's or employer's written confirmation.

SFIs should refer to the full list of several sources that can be used (see the Category C documents set out in Appendix B).

68 Each SFI must develop internal policies and procedures to quickly and securely authenticate electronic contact information. Some forms of contact, such as a mobile phone number or email address, can be authenticated almost immediately.

69 Nationality should be established to ensure that the facility holder is not from a nation that is subject to sanctions by the United Nations or similar prohibition from an official body or government. This would prohibit such business being transacted. (SFIs should refer to Appendix C for a list of websites which contain information on sanctions).

70 Obtaining a customer's date of birth provides an extra safeguard. For example, when a forged or stolen passport or driver's license bears a date of birth that is clearly inconsistent with the age of the person presenting the document.

71 Information and documentation must be obtained and retained to support or evidence the details provided by the facility holder.

72 Identification documents, whether provided as originals or certified copies (including certified digital copies), should be pre-signed. SFIs may require one of the identification documents obtained to include a photograph. However, there are numerous other reliable sources that SFIs may utilize to verify customer information. Therefore, SFIs should not mandate that all identification documents include a photograph. SFIs should exercise sound judgement when dealing with minors and other individuals who have a legitimate reason for lacking photo identification (see Appendix B – *How to Identify Minors*). When a document bears a photograph, it must be clearly discernible

73 Where prospective customers provide documents with which a SFI is unfamiliar, either because of origin, format or language, the SFI must take reasonable steps to verify that the document is indeed authentic, which may include contacting the relevant authorities or obtaining a notarized translation.

A2. When is Further Verification of Identity Necessary?

74 Regulation 12 of the FTRR addresses continued verification of accounts. It provides that where the identity of a facility holder has been verified, no further verification of identity is necessary **unless** there is a material change in the operation of the facility. For example, the re-verification process should not be triggered solely by the expiration of existing documentation.

A material change in the operation of a facility includes, but is not limited to:

- a change in the ownership of the facility; or
- activities which give rise to the suspicion of any identified risk

Where a customer's identity has been verified, further verification is also mandatory if during the course of the business relationship the SFI has reason to doubt the veracity or adequacy of previously obtained identification information of the customer.

In such cases, verification should take place before the facility holder conducts any further business.

75 In conducting the re- verification exercise, SFIs should have regard to the fact that the purpose of re- verifying a customer's identity is to enable law enforcement to have access to the appropriate identification documentation and information.

76 SFIs may also as part of their own internal AML/CFT/CPF and KYC policies, re- verify a customer's identity on the occurrence of any of the following "trigger events":

(i) a significant transaction (relative to a relationship);

(ii) a material change in the operation of a business relationship;

(iii) a transaction which is out of keeping with previous activity;

(iv) a new product or account being established within an existing relationship;

(v) a change in an existing relationship which increases a risk profile (as stated earlier); and

(vi) the assignment or transfer of ownership of any product.

The above list should not be considered exhaustive.

77 The need to confirm and update information about identity, and the extent of additional KYC information to be collected over time will vary between SFIs. It will also depend on the nature of the products or services being offered, and whether personal contact is maintained, enabling file notes of discussions to be made; or whether all contact with the customer is remote.

A3. Persons without Standard Identification Documentation

78 Most people interact with the formal financial system at some point in their lives. It is important, therefore, that certain groups are not precluded from obtaining financial services solely because they do not possess the usual evidence of identity or address. Especially when they cannot reasonably be expected to do so. The elderly, persons with disabilities, students, minors, and

the socially or financially disadvantaged are most likely to experience these difficulties.

79 Internal procedures must provide appropriate advice to staff on how identity can be confirmed in those exceptional circumstances where a manager may authorise the opening of a facility without the usual documentation. The decision leading to the authorization must be recorded on the customer's file. SFIs must retain this information in the same manner and for the same period of time as other identification records.

80 In particular, domestic SFIs should exercise discretion and flexibility without compromising sufficiently rigorous AML/CFT/CPF procedures. This flexibility is especially relevant to provide appropriately defined and limited services to certain types of customers (for example, to increase customer access for financial inclusion purposes).

81 In some cases, it may be possible for the SFI to accept confirmation from a suitable referee: a person ordinarily resident in The Bahamas who knows the customer, and can be relied upon to confirm that the customer is who he or she claims to be. SFIs should refer to Appendix B for further guidance on who would be considered a suitable referee.

82 For students or other young people, the normal identification procedures set out above should be followed as far as possible. However, SFIs should be mindful that registration fraud is known to occur at the beginning of the academic year before students have taken up residence at their place of education.

83 In most cases, a minor is introduced by a family member or guardian who has a pre-existing relationship with the SFI concerned. In cases where the person opening the account is not already known, the identity of that person, and any other person who will have control of the account, should be verified.

A4. Certification of Identification Documents

84 SFIs should exercise caution when considering certified copy documents, especially where such documents originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction. Where certified copy documents are accepted, it is the SFI's responsibility to satisfy itself that the certifier is appropriate. In all cases, SFIs should also ensure that the customer's signature on the identification document matches the signature on the application form, mandate, or other document.

85 In the case of natural persons, where face-to-face customers show SFIs' staff original documents bearing a photograph, copies should be taken immediately, retained and certified by a senior staff member**.**

86 Where it is impractical or impossible to obtain sight of original documents, a copy is acceptable where it has been certified by a suitable certifier as being a true copy of the original document and that the photo is a true likeness of the facility holder.

87 A certifier must be a suitable person; such as those below. The following list of suitable certifiers *is not intended to be exhaustive*, nor are SFIs required to accept all of them:

- certified public accountant;
- bank or trust company official;
- counsel and attorney-at-law;
- senior civil servant;
- doctor of medicine;
- justice of the peace;
- member of the House of Assembly;
- minister of religion;
- notaries public;
- police officer;
- teacher; or
- corporate secretary.

88 The certifier should sign the copy document, print/indicate his name clearly underneath, and clearly indicate his position or capacity on it together with a contact address, telephone and facsimile number and where applicable, a license/registration number.

B. Corporate Clients

89 SFIs must obtain the following documents and information when seeking to verify the identity of corporate clients:

(i) The original or a certified copy of the Certificate of Incorporation or equivalent document;

(ii) certified copy of the Memorandum and Articles of Association;

(iii) name and location of the registered office and registered agent of the corporate entity, where appropriate, or if different, location of principal place business;

(iv) description and nature of the corporate entity's business including:

(a) date of commencement of business;
(b) products or services provided; and

(c) location of principal business;

(vi) a copy of the Board Resolution authorising the opening of the account or other facility and the signatories authorized to sign on the account;

(vii) satisfactory evidence of the identity of all account signatories, details of their relationship with the company and if they are not employees an explanation of the relationship. All signatories must be verified in accordance with Appendix B and paragraphs 61(i) – (iii) and 62(i) and (ii) of these Guidelines;

(viii) satisfactory evidence of the identity of each of the natural person(s) (a) with a controlling interest in the corporate entity (other than a publicly traded company), being any person holding an interest of 10% or more or with principal control over the company's assets, (b) who otherwise exercises control over the management of the corporate entity, and (c) where no natural persons are identified under subparagraph (a) or (b), the identity of the natural person(s) who holds the position of senior managing official(s). The identities of all persons referred to in (a) and (b) must be verified in accordance with Appendix B and paragraphs 61(i) – (iii) and 62(i) and (ii) of these Guidelines; and

(ix) confirmation before a business relationship is established, by way of company search and/or other commercial enquiries, that the applicant company has not been, or is not in the process of being, dissolved, struck off the companies register, wound-up or terminated. Such confirmation may be verified by obtaining a current Certificate of Good Standing or equivalent document or alternatively, obtaining a set of consolidated financial statements that have been audited by a reliable firm of auditors and that show the group structure and ultimate controlling party.

90 In addition, SFIs should obtain the following information and documents when seeking to verify the identity of corporate clients:

(i) the reason for establishing the business relationship;

(ii) the potential parameters of the account including:

(a) size in the case of investment and custody accounts;

(b) balance ranges, in the case of current and deposit accounts;

(c) an indication of the expected transaction volume of the account;

(d) the source of wealth in circumstances where the SFI's customer is considered a high-risk client;

(e) the source of funds; and

(f) a copy of the last available financial statements where appropriate;

(iii) copies of Powers of Attorney, or any other authority, affecting the operation of the account given by the directors in relation to the company and supported by a copy of the respective Board Resolution;

(iii) copies of the list/register of directors and officers of the corporate entity including their names and addresses;

(iv) written confirmation that all credits to the account are and will be beneficially owned by the facility holder except in circumstances where the account is being operated by an intermediary for the purpose of holding funds in his professional capacity;

(v) satisfactory evidence of identity must be established for at least two (2) directors, one of whom should, if applicable, be an executive director where different from account signatories; and

(vi) such other official documentary and other information as is reasonably capable of establishing the structural information of the corporate entity.

91 It is sometimes a feature of corporate entities being used to launder money or finance terrorism that account signatories are not directors, managers or employees of the corporate entity. In such circumstances, SFIs should exercise caution, making sure to verify the identity of the signatories in accordance with Appendix B and paragraphs 61(i)-(iii), 62(i) and (ii) and where appropriate, monitor the ongoing business relationship more closely.

92 Where it is impractical or impossible to obtain sight of original incorporation documents, SFIs may accept a suitably certified copy in accordance with the procedures stated in paragraphs 84 to 87 of these Guidelines.

93 Trading companies may sometimes form part of complex organisational structures which also involve trusts, executive entities and foundations. Particular care should be taken to verify the existence of any legal entity and to ensure that any person purporting to act on its behalf is authorised to do so. The principal requirement is to look behind a legal entity to identify those natural persons who have ultimate control over the business and the entity's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the entity. Enquiries should be made to confirm that the legal entity exists for a legitimate trading or economic purpose, for example SFIs may, where appropriate visit the business/company to ensure that there is an actual physical presence.

94 In addition, if the SFI becomes aware of changes in the company structure or ownership, or suspicions are aroused by a change in the nature of business transacted, further checks should be made.

95 Where the business relationship is being opened in a different name from that of the corporate entity, the SFI should make a search, for both names.

96 Where persons are already known to the SFI and identification records are already in compliance with the requirements of these Guidelines, there is no need to verify identity again.

97 When authorised signatories change, care should be taken to ensure that the identities of all current signatories have been verified. In addition, it may be appropriate to make periodic enquiries to establish whether there have been any changes in directors/shareholders, or the nature of the business/activity being undertaken. Such changes could be significant in relation to potential money laundering or terrorist financing activity, even though authorised signatories have not changed.

C. Segregated Accounts Companies

98 Where the corporate client is a segregated accounts company, SFIs should have regard to the guidance for corporate clients (paragraphs 89 to 97). In addition to the documents and information set out in paragraphs 89 and 90, SFIs should also obtain a copy of the Registrar General's certificate of registration to confirm the existence and legal standing of the segregated accounts company.

D. Powers of Attorney

99 The authority to deal with assets under a power of attorney constitutes a business relationship. Therefore, where appropriate, SFIs should verify the identities of holders of powers of attorney, the grantor of the power of attorney and third-party mandates in accordance with paragraph 61 and 62 and Appendix B. Records of all transactions undertaken in accordance with a power of attorney should be kept in accordance with Section VII of these Guidelines.

E. Partnerships and Unincorporated Businesses

100 SFIs must obtain the following documents and information when seeking to verify the identity of partnerships and unincorporated businesses:

(i) identification evidence for all partners/controllers or beneficial owners of a firm or business and the natural person(s) who holds the position of

senior managing official(s), in line with the requirements in these Guidelines for individual customers (see Appendix B and paragraphs 61 to 63).

(ii) identification evidence for all authorised signatories, in line with the requirements in these Guidelines for individual customers (see Appendix B and paragraphs 61 to 63). When authorised signatories change, care should be taken to ensure that the identity of the current signatories has been verified;

(iii) a copy of the partnership agreement (if any) or other agreement establishing the unincorporated business; and

(iv) a mandate from the partnership or beneficial owner authorising the opening of an account or the use of some other facility and conferring authority on those who will undertake transactions should be obtained.

101 When partners/controllers change, care should be taken to ensure that the identities of the new partners/controllers are verified.

102 The following information should also be obtained when SFIs seek to verify the identity of partnerships and unincorporated businesses:

(a) description and nature of the business including:

i. date of commencement of business;

ii. products or services provided; and

iii. location of principal place of business;

(b) the reason for establishing the business relationship and the potential parameters of the account including:

i. size in the case of investment and client accounts;

ii. balance ranges, in the case of deposit and client accounts;

iii. an indication of expected transaction volume of the account;

iv. the source of wealth in circumstances where the SFI's customer is considered a high-risk client;

v. the source of funds;

vi. a copy of the last available financial statements where appropriate;

vii. written confirmation that all credits to the account are and will be beneficially owned by the facility holder except in circumstances where the account is being operated by an intermediary for the purpose of holding funds in his professional capacity; and

viii. such documentary or other evidence as is reasonably capable of establishing the identity of the partners or beneficial owners.

F. Financial and Corporate Service Providers

103 SFIs are required to verify the identity of financial and corporate service providers ("FCSPs") licensed under the Financial and Corporate Service Providers Act, 2000 ("the FCSPA"). SFIs should also, in accordance with the FTRA, verify the identity of any clients of an FCSP where the FCSP operates a facility, such as for example, an omnibus account, on behalf of its clients.

104 In the case of FCSPs, SFIs should adhere to the following guidance when conducting due diligence on a FCSP or their underlying clients:

(i) where a FCSP or their underlying clients are natural persons, SFIs should follow the guidance set out in Appendix B and paragraphs 61 to 73;

(ii) where a FCSP or their underlying clients are companies, SFIs should follow the guidance set out in paragraphs 89 to 97, and

(iii) where a FCSP is or their underlying clients are partnerships or unincorporated associations, SFIs should follow the guidance set out in paragraphs 100 to 102.

105 In each case, a copy of the FCSP's licence and a Certificate of Good Standing from the Registrar of Companies should be obtained in order to confirm the existence and legal standing of the FCSP.

G. Other Legal Structures and Fiduciary Arrangements

106 Legal structures such as trusts, foundations, Executive Entities and any other legal arrangements (recognised under Bahamian Law), may be misused to conceal illicit funds where the trustee, protector, settlor, or any person with ultimate effective control is not subject to adequate KYC/CDD procedures. For the purposes of these Guidelines, where applicable, SFIs should also have regard to the potential misuse of similar legal arrangements with customers from civil

law jurisdictions including fiducie, certain types of Treuhand, fideicomiso and Waqf (in line with its definition in the FATF Glossary)[10].

107 In relation to Trustees and Trust Corporate Service Providers (TCSPs) acting for non-Exempted Clients (see paragraphs 162-164) or non-Eligible Introducers (see paragraphs 151–152), SFIs must apply enhanced due diligence commensurate with risk and ensure that all individuals with ultimate effective control are identified, verified, and their interest documented. The primary means of preventing misuse is verification of the identity of all persons who, directly or indirectly, hold ultimate effective control over the funds or assets, including the settlor, trustees, protectors, advisers, corporate service providers acting in a fiduciary capacity, and any other individuals who hold power to remove trustees/advisors, or otherwise influence the disposition of trust property, alter, or benefit from the trust or foundation.

108 In addition to obtaining identification evidence for the trustee(s) and any other signatories on the account SFIs must, verify the identity of:

(i) the settlor(s), the protector (if any) and such other person(s) exercising ultimate effective control over the trust which includes an individual who has the power (whether exercisable alone, jointly with another person or with the consent of another person) to—

(a) dispose of, advance, lend, invest, pay or apply trust property;

(b) vary the trust;

(c) add or remove a person as a beneficiary or to or from a class of beneficiaries;

(d) appoint or remove trustees;

(e) direct, withhold consent to or veto the exercise of a power such as is mentioned in subparagraph (a), (b), (c) or (d); and

(ii) any other TCSPs, or other regulated agents serving the trust, and any other service providers to the trust, including investment advisors or managers, accountants, and tax advisors and ensure that such information is kept accurate, up to date and re-verified upon material changes to control, ownership, or management.

[10] FATF Glossary Definition of "Legal Arrangements" https://www.fatf-gafi.org/en/pages/fatf-glossary.html#accordion-a13085a728-item-

109 Identity verification information must be documented and where applicable corroborated from independent sources.

110 SFIs must also ensure that all identification information obtained is kept up-to-date, and in conformity with these Guidelines in addition to the on-going verification requirements under the Register of Beneficial Ownership Act, 2018 ("ROBO Act") as amended.

111 In the case of ~~a~~ nominee arrangements, SFIs must obtain identification evidence for the beneficial owner(s). For TCSPs and trustees acting as nominees the term 'beneficial owner' includes any natural person who ultimately owns or controls either the settlor, the beneficiary, or the nominee arrangement, and any individual who ultimately has the power to dispose of or benefit from the assets held in the trust or foundation. For the purpose of these Guidelines and consistent with the latest legislative amendments, where shares or other interests are held by a nominee, the person on whose behalf the nominee acts shall be treated as the beneficial owner and must be verified in accordance with sections 8 and 9 of the ROBO Act as amended.

112 For example, in nominee shareholder relationships, the existence of the nominee shareholder arrangement must be expressly stated in the company's memorandum and recorded on the register of members pursuant to section 29A of the International Business Companies Act as amended and section 9A of the Companies Act as amended. The nominee must execute a declaration of trust naming all beneficiaries and such declaration must be maintained at the company's registered office. These requirements apply equally to domestic companies and international business companies.

113 Notwithstanding the existence of a declaration of trust, all nominee shareholders are further required to:

(a) disclose the identity and relevant particulars of the person or persons on whose behalf they hold shares in accordance with section 29 of the IBC Act, section 9 of the Companies Act, and sections 8 and 9 of the ROBO Act; and
(b) provide all required particulars for the legal entity and its registered agent in compliance with sections 8 and 9 of the ROBO Act.

114 SFIs must ensure that such beneficial ownership information obtained is adequate, accurate and kept up to date, and the information obtained is verified and adequate records maintained and are available for the competent authority in a timely manner, as requested.

115 In addition to obtaining identification information, SFIs should conduct appropriate inquiries to understand the intended nature and the purpose of the legal structure and the source of funds.

116 Where the settlor is deceased, written confirmation should be obtained for the source of funds, for example, Grant of Probate, and/or copy of the Last Will and Testament creating the trust, and the executor/administrator's identity verified, where applicable.

117 Where a corporate trustee acts jointly with a non-regulated co-trustee, the identity of any non- regulated co-trustees should be verified even if the corporate trustee is covered by an exemption. The relevant guidance contained in this section for verifying the identity of natural persons, unincorporated associations or companies should be followed.

118 Copies of any documents should be certified as true copies. In addition, a cross check should be made to ensure that any bank account on which the trustees have drawn funds is in their names, and the identities of any additional signatories verified.

Trustees and persons acting in a nominee capacity should disclose their status as trustees and nominees to financial institutions when forming a business relationship or carrying out occasional transactions. Any application to open an account, or undertake a transaction, on behalf of another without the applicant identifying a trust or nominee capacity should be regarded as suspicious and should trigger further enquiries under The Bahamas AML/CFT/CPF regime. Documentation of such disclosures and any follow-up actions should be maintained for a minimum period of five (5) years following termination of the business relationship.

119 Additionally, as required by Section 15 of the FTRA, Trustees and persons acting in a nominee capacity must maintain the information referred to above for at least five (5) years after the business relationship has ended. Trustees and persons acting in a nominee capacity are required to cooperate, to the fullest extent possible, with competent authorities in providing necessary information relating to the trust or legal arrangement.

120 SFIs are also legally required by the FTRA (see section 7) and the ROBO Act as amended to verify the identity of any underlying beneficiary of a legal structure (see section 7). During the onboarding process, it may not always be possible to identify the beneficiaries of trusts precisely. For example, some beneficiaries may be unborn children and some may only become vested on the occurrence of specific events.

Where the beneficiary has a vested interest in the legal structure, the SFI providing the facility must conduct verification procedures unless the transaction is, or has been introduced by, another financial institution on behalf of the settlor and beneficiary and such financial institution is itself required to verify the identity of the settlor and beneficiary. See the section *"Reliance on*

Third Parties to Conduct KYC on Customers" for further guidance. Verification must be conducted prior to making a distribution to the beneficiary or when the beneficiary intends to exercise vested rights.

121 SFIs should be particularly vigilant where there is no readily apparent connection or relationship between the settlor and the beneficiaries of a trust. SFIs should endeavour, as much as possible, to ascertain the settlor's reasons for wanting to benefit a beneficiary with whom there is no obvious connection. This can be a matter of great sensitivity, and SFIs are encouraged to pursue appropriate inquiries and maintain a documented record of the rationale and actions taken, while protecting data privacy.

122 The appointment or use of nominee directors is expressly prohibited under section 41A of the IBC Act, (as amended) and section 80A of the Companies Act (as amended). A person shall not serve or be appointed as a director if acting pursuant to any agreement, arrangement, or understanding whether formal or informal, expressed or implied. A person shall also not act in accordance with the instructions, direction, influence, or wishes of another person relative to the exercise of their duties or powers as a director

123 Any person who acts as, or who causes or permits the appointment of a nominee director, commits an offence and is liable on summary conviction to a fine up to $50,000, imprisonment for a term not exceeding 12 months or both. Companies both domestic and international that knowingly retain a nominee director are subject to civil penalties of up to $1,000 per day for each day that the breach continues.

124 Companies have been afforded a six-month transitional period following the commencement of the 2025 amendments to the IBC Act and Companies Act, to cease the appointments of nominee directors and regularise their governance arrangements. During this period, companies are required to cease the appointment or use of nominee directors and to file the requisite declaration with the Registrar confirming that any nominee directorship had been terminated within the prescribed timeframe.

H. Identification of New Trustees

125 Where a Trustee is replaced, due diligence must be conducted and the identity verified before the new trustee is allowed to exercise control over trust assets. When a trustee is replaced, the SFI is expected to document the justification for the replacement, maintain adequate, accurate and up-to date due diligence documentation for the new of Trustee, to ensure such information may be made available to competent authorities in a timely manner, if requested. Documentation should be maintained for a minimum period of five (5) years following termination of the business relationship.

126 A change in trustee also constitutes a material change triggering reassessment of the risk profile of the legal arrangement.

I. Foundations

127 For transparency and beneficial ownership information purposes, foundations should be treated in a manner comparable to trusts and other legal arrangements with equivalent obligations regarding the collection, maintenance and availability of adequate, accurate and up-to-date- beneficial ownership information.

128 SFIs should obtain the following information concerning foundations:

(i) the foundation's charter;

(ii) the Registrar General's certificate of registration or document of equivalent standing in a foreign jurisdiction (to confirm the existence and legal standing of the foundation);

(iii) document information on the source of funding for the foundation. In cases where a person other than the founder provides funds for the foundation, SFIs should verify the identity of that third party and/or for whom a founder may be acting in accordance with paragraphs 61 to 73 and Appendix B of these Guidelines; and

(iv) identification evidence for the founder(s) and for such officers and council members of a foundation as may be signatories for the account(s) of the foundation. SFIs should follow the guidance in Appendix B and paragraph 61(i) – (iii), 62(i) and (iii) when verifying the identities of signatories. Where the founder is a company, SFIs should have regard to the guidance on corporate clients contained in paragraphs 102 to 110; where the founder is an individual, SFIs should follow the guidance provided in Appendix B and paragraphs 73 to 85.

129 Identification evidence should also be obtained and verified for all vested beneficiaries of the foundation.

J. Executive Entities

130 In accordance with the BTCRA[11], executive entities exercising the powers and duties of trustees are under the regulatory oversight of the Central Bank and are considered legal arrangements for the purposes of these Guidelines. As such, executive entities must conform to the obligations regarding the

[11] See the Banks and Trust Companies (Amendment) Act, 2025

collection, maintenance and availability of adequate, accurate and up-to-date- beneficial ownership information as required for trustees.

131 For further guidance SFIs may also refer to the Central Bank's "*General Information and Application Guidelines For Private Trust Companies, Qualified Executive Entities And Their Registered Representatives"*, issued on the 21 November, 2025.

K. Executorship Accounts

132 Where a business relationship is entered into for the purpose of winding up the estate of a deceased person, the identity of the executor(s)/administrator(s) of the estate should be verified in line with this guidance, depending on the nature of the executor (i.e. whether personal, corporate, or a firm of attorneys). However, the identity of the executor or administrator need not normally be verified when payment from an established bank account in the deceased's name is being made to the executor or administrator in accordance with the Grant of Probate or Letters of Administration solely for the purpose of winding up the estate. Payments to the underlying beneficiaries on the instructions of the executor or administrator may be made without verification of their identity.

133 If any suspicions are aroused about the nature or origin of assets comprising an estate that is being wound up, then a report of the suspicions should be made to the FIU in accordance with the procedures set out in the FIU's Suspicious Transactions Reporting Guidelines.

L. Non-Profit Associations (Including Charities)

134 Non-profit associations may pose risks of money laundering or terrorist financing for SFIs. At the placement stage there may be difficulties in identifying the source of funds, the identity of the donor, and verifying the information where it is provided. In some circumstances, such as in the case of anonymous donations, the identity of the donor is unknown and as a result neither is the source of the funds.

135 Where the non-profit association is a corporate entity the account opening procedures should be in accordance with the procedures for corporate clients set out in paragraphs 89 to 97 in the case of trusts the procedures in paragraphs 106 to 124; in the case of foundations the procedures in paragraphs 127 and 129 should be followed.

136 Where a facility holder is a non-profit association, it will normally be necessary to obtain the following documented information:

(i) an explanation of the nature of the proposed entity's purposes and operations; and

(ii) the identity of at least two signatories and/or anyone authorized to give instructions on behalf of the entity should be obtained and verified.

137 Where a non-profit association is registered as such in an overseas jurisdiction, it may be useful for the SFI to contact the appropriate overseas charity commission or equivalent body, to confirm the registered number of the charity and to obtain the name and address of the commission's correspondent for the charity concerned. SFIs should satisfy themselves as to the legitimacy of the organization by, for example, requesting sight of the constitution.

138 SFIs should refer to Appendix B for a list of relevant websites providing information on non-profit organizations and charities.

139 Whilst it is impractical to obtain documentary evidence of identity of all donors, SFIs should undertake a basic "vetting" of all non-profit associations established in other jurisdictions, in relation to known money laundering and terrorist activities. This includes a reasonable search of public information, verifying that the non-profit association does not appear on any terrorist lists nor that it has any association with money laundering and that identification information on representatives /signatories is obtained. Particular care should be taken where the associations' funds are used for projects located in high-risk jurisdictions (see paragraphs 183 and 184 below).

M. Products and Services Requiring Special Consideration

140 Special consideration should be given to the provision of the following products and services:

(a) Provision of Safe Custody and Safety Deposit Boxes

141 Where facilities to hold boxes, parcels and sealed envelopes in safe custody are made available, it is expected that SFIs will follow the identification procedures set out in these Guidelines.

(b) Intermediaries

142 SFIs are required to not only verify the identity of an intermediary but also to look through that entity to the underlying client(s) where the intermediary is not one of the financial institutions referred to in paragraphs 152 and 153 of these Guidelines. and/or is from a country that is not subject to AML/CFT/CPF

obligations, under supervision for compliance with those obligations, and has inadequate procedures for compliance with customer due diligence and record keeping requirements. In these circumstances, measures must be taken to verify the identity of the underlying clients. In satisfying this requirement, the SFI should have regard to the nature of the intermediary, the domestic regulatory regime in which the intermediary operates, to its geographical base and to the type of business being done. Where however, the intermediary is one of the financial institutions referred to in paragraph 152 and 153, such verification is not required.

(c) Occasional Transactions

143 It is important for SFIs to determine whether a facility holder is undertaking an occasional transaction, or whether the transaction is the initial step in an ongoing business relationship as this can affect the verification requirements. The same transaction may be viewed differently by a SFI, and by an introducing intermediary, depending on their respective relationships with the facility holder. Therefore, where a transaction involves an intermediary, both the SFI and the intermediary must separately consider their positions, and ensure that their respective obligations regarding verification of identity and associated record keeping are met.

144 The FTRA defines an "occasional transaction" as any one-off transaction or linked transactions, that are carried out by a person otherwise than through a facility in respect of which that person is a facility holder.

145 SFIs must verify the identity of customers who conduct occasional transactions (whether a single transaction or a series of linked transactions).

146 As a matter of best practice, a time period of 3 months for the identification of linked transactions is normally acceptable. However, there is some difficulty in defining an absolute time scale that linked transactions may fall within. Therefore, the relevant procedures for linking will ultimately depend on the characteristics of the product rather than relating to any arbitrary time limit. For example, SFIs should be aware of any obvious connections between the sender of funds and the recipient.

RELIANCE ON THIRD PARTIES TO CONDUCT KYC ON CUSTOMERS

147 Every SFI must retain adequate documentation to demonstrate that its KYC procedures have been properly implemented, and that it has carried out the necessary verification procedures.

148 In certain circumstances, it may be possible for SFIs to rely on KYC procedures carried out by other financial institutions.

Examples of such circumstances are:

(i) where a SFI is unable to readily determine whether or not an occasional transaction involves cash because a customer deposited funds into a facility held for and on behalf of the SFI by another financial institution; or

(ii) where a financial institution being a facility holder of the SFI, conducts a transaction on behalf of a customer, using the facilities of a SFI, the SFI may rely upon the written confirmation of the financial institution that it has verified the identity of the customer concerned.

149 Where such transactions are conducted, in addition to obtaining written confirmation, a SFI must also confirm the existence of the facility provided by the financial institution.

150 This exemption applies only to occasional transactions and transactions conducted by financial institutions that are facility holders of SFIs. However, if the person on whose behalf the transaction is being conducted is being introduced to the SFI for the purpose of forming a business relationship with the SFI, then that SFI must carry out the appropriate due diligence and obtain the necessary evidence of identity, subject to the provisions in the section on *Introductions from Group Companies or Intermediaries.*

Introductions from Group Companies or Intermediaries

151 Where a business relationship commences, the SFI is obligated to carry out KYC procedures on any client introduced to it by another financial institution, unless the financial institution is an eligible introducer.

152 To be an eligible introducer for a SFI, the Central Bank requires that a domestic financial institution must be one of the following regulated financial institutions:

(i) A, bank, trust company, or credit union regulated by the Central Bank;

(ii) a company carrying on life assurance business pursuant to section 2 of the Insurance Act;

(iii) a broker dealer, registered under the Securities Industry Act 2024; or

(iv) an investment fund administrator licensed under the Investment Funds Act, 2019).

153 A foreign financial institution may also qualify to act as an eligible introducer if it meets all three of the following conditions:

(i) it must exercise functions similar to those of the financial institutions listed in sub-paragraphs 152 (i) to (iv) above and be based in a country that is subject to AML/CFT/CPF obligations, is under supervision for compliance with those obligations, and which has adequate procedures for compliance with customer due diligence and record keeping requirements;

(ii) it must be subject to equivalent or higher AML/CFT/CPF standards of regulation as provided for in Bahamian law; and

(iii) there must be no obstacles which would prevent the SFI from obtaining the original documentation.

154 From time to time, the Minister may by notice designate any jurisdiction that he considers fulfils the terms of sub-paragraph 153 (i). In this regard, the Minister may take into consideration the level of the country risk associated with the jurisdiction. SFIs are therefore required to report to the Central Bank and to the IRF Steering Committee where there has been persistent regulatory failure of which they are aware, in respect of the identified risk framework or recognized weak compliance with international CDD requirements by any jurisdiction or foreign financial institution (see section 9 of the FTRA).

155 A third party can act as an eligible introducer when the above criteria have been met, provided there is no suspicion of breach of the identified risk framework, or the commission by the facility holder of any offence designated as an identified risk.

156 A SFI may rely upon the customer due diligence measures carried out by the eligible introducer but remains ultimately responsible for ensuring that adequate due diligence procedures are followed, and that the documentary evidence being relied upon is satisfactory for these purposes. Evidence is considered satisfactory if it shows that the eligible introducer is subject to AML/CFT/CPF regulatory standards that are equivalent to, or higher than, those provided under Bahamian law. Only senior management should make the decision to rely upon the eligible introducer. The basis for deciding that normal due diligence procedures need not be followed should be part of the SFI's risk-based assessment.

157 SFIs should ensure that they immediately obtain all the relevant information pertaining to a customer's identity. The Central Bank will also require that SFIs have clear and legible copies of all documentation in their possession within 30 days of receipt of the written confirmation of the eligible introducer that they have verified customer identity in accordance with their national laws. The

eligible introducer must certify that any photocopies forwarded are identical with the corresponding originals. This certification should be provided by a senior member of the introducer's management team and may be endorsed on the written confirmation (that a client's identity has been verified) provided by the introducer. If documents are not obtained within 30 days of receipt of the introducer's written confirmation, the account should be suspended and if after a further reasonable period, the SFI still does not receive the documents, the business relationship must be terminated.

SIMPLIFIED DUE DILIGENCE

158 The obligation to maintain procedures for obtaining evidence of identity is general, but paragraphs 158.1 to 162 set out a number of exemptions and concessions.

158.1 In accordance with section 7 of the FTRA, where the risks identified are low, a SFI is permitted to conduct simplified due diligence measures, unless there is a suspicion of activities related to any identified risk. This determination should be based on the risk assessment described in section 5 of the FTRA. Where a SFI has made the decision to apply simplified CDD measures, it must retain documentation that supports the basis for the decision.

A. Bahamian or Foreign Financial Institutions

159 Verification of identity is not normally required when the facility holder is one of the financial institutions referred to in paragraphs 152 or 153. SFIs should satisfy themselves that the financial institution does actually exist (e.g. that it is listed in the Bankers' Almanac, or is a member of a regulated or designated investment exchange); and that it is also regulated and subject to equivalent or higher AML/CFT/CPF standards of regulation as provided for in Bahamian law.

160 In all cases, the SFI must be satisfied that it can rely upon the eligible introducer. The SFI should request from an eligible introducer such evidence as it reasonably requires to satisfy itself as to the identity of the introducer and the robustness of its KYC policies and procedures.

161 Other Bahamian or foreign financial institutions (e.g. bureaux de change) should be subject to further verification in accordance with the procedures for companies or businesses.

B. Exempted Clients

162 In accordance with regulation 8 of the FTRR, documentary evidence of identity will not normally be required in the case of:

(i) financial institutions regulated by the Central Bank of The Bahamas, the Securities Commission of The Bahamas, the Insurance Commission of The Bahamas, the Inspector of Financial and Corporate Services or the Gaming Board;

(ii) financial institutions which are subject to AML/CFT/CPF obligations, are under supervision for compliance with those obligations and which have adequate procedures for compliance with CDD and record keeping requirements;

(iii) any central or local government agency or statutory body; and

(iv) a publicly traded company or investment fund listed on The Bahamas International Stock Exchange or any other Stock Exchange specified in the Schedule to the FTRR and approved by the Securities Commission.

163 In accordance with the provisions of the Payments Instruments (Oversight) Regulations, 2017, Payments Institutions may waive customer identification procedures when the Bahamian dollar electronic payment instrument has an initial maximum stored limit of B$500, and is reloadable up to a maximum value of B$300 per month. If at the time of issuance, an electronic payment instrument immediately (or prospectively) falls outside of these parameters, the customer identification and verification provisions of Appendix B apply.

164 Irrespective of the size and nature of the transactions or proposed transactions and exemptions set out above, identity must be verified in all cases where:

(a) there is a suspicion of activities relating to identified risks involving the facility holder or the facility holder's account or,

(b) if, during the course of the business relationship, the SFI has reason to doubt the veracity or adequacy of previously obtained identification information of the customer.

If activities related to identified risks are known or suspected then a report must be made to the FIU. Knowledge or suspicion of offences under the ATA must be reported to the police. In both cases, verification must take place before the facility holder may conduct any further business.

ENHANCED DUE DILIGENCE

165 SFIs should apply enhanced CDD measures on a risk sensitive basis for those categories of business relationships or transactions with a facility holder, beneficial owner or financial institution which the SFI has determined present a

higher risk for money laundering or terrorist financing or are from a jurisdiction assessed as higher risk by the IRF Steering Committee (see section 13 of the FTRA and section 6(3) of the POCA), or where there is a suspicion of activities related to any identified risk (see section 7 of the FTRA). As part of this, a SFI may conclude, using a risk-based approach, that the standard evidence of identity (see paragraphs under section IDENTIFICATION PROCEDURES) is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer.

166 The extent of additional information sought, and of any monitoring carried out in respect of any particular customer, or class/category of customer, will depend on the money laundering or terrorist financing risk that the customer, or class/category of customer, is assessed to present to the SFI. A SFI should retain a fuller set of information in respect of those customers, or class/category of customers, assessed as carrying a higher money laundering or terrorist financing risk, or who are seeking a product or service that carries a higher risk of being used for money laundering or terrorist financing purposes.

167 SFIs should give particular attention to the following business relations and transactions:

(a) where the customer has not been physically present for identification purposes (see the following paragraphs on *Transactions by Non-Face-to-Face Customers*);

(b) correspondent banking relationships (see the following paragraphs on *Correspondent Relationships);*

(c) a business relationship or occasional transaction with a PEP (see the following paragraphs on *Politically Exposed Persons*).

(d) business relations and transactions with natural or legal persons from, or in, countries and jurisdictions known to have inadequate AML/CFT/CPF measures including, in all cases, those countries which the Financial Action Task Force (FATF) has identified as high-risk or non-cooperative (see the following paragraphs on *High-Risk Countries).*

(e) corporate clients able to issue bearer shares or bearer instruments (see the following paragraphs on *Bearer Shares).*

A. Transactions by Non-Face-to-Face Customers

168 SFIs should consider the specific risks posed when establishing business relations, undertaking transactions and conducting ongoing customer due

diligence where there is no face-to-face contact with the customer or the prospective customer.

169 Non-face-to-face transactions carry an inherent risk of forgery and fraud. SFIs should mitigate these risks with their internal systems, policies and procedures. The CDD measures taken by a SFI in respect of non-face-to-face customers will depend on the nature and characteristics of the product or service provided, and the customer's risk profile.

170 Where verification of identity is performed without face-to-face contact, a SFI should take specific and adequate measures to compensate for the resultant higher risk. A SFI may apply one or more of the following measures:

(a) requiring the customer's first payment or transaction to be carried out through an account in the customer's name with a Bahamian financial institution or a financial institution located in a country which is subject to AML/CFT/CPF obligations, is under supervision for compliance with those obligations, and has adequate procedures for compliance with customer due diligence and record keeping requirements;

(b) requiring additional documents to complement those required for face-to-face customers;

(c) making telephone contact with the customer on a home or business number which has been verified prior to opening an account or conducting a transaction;

(d) communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, might be required to be returned completed or acknowledged without alteration);

(e) internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address; and

(f) requiring copy documents to be certified by a suitable certifier.

171 File copies of supporting evidence must be retained. SFIs that regularly conduct one-off transactions should record the details in a manner which allows cross reference to transaction records. Such SFIs may find it convenient to record identification details on a separate form, to be retained with copies of any supporting material obtained.

172 An introduction from a respected customer personally known to the SFIs management, or from a trusted member of staff, may assist the verification procedure but does not replace the need for verification of identity as set out above. Details of the introduction should be recorded on the customer's file.

B. Correspondent Relationships

173 For the purposes of this section –

"correspondent relationship" means the provision of banking, payment, cash management, international wire transfers, cheque clearing, payable through accounts, foreign exchange, securities transactions, cash transfers or similar services by one financial institution (the 'correspondent institution'), to another financial institution (the 'respondent institution');

174 When entering into a correspondent relationship, in addition to applying the measures under sections 6 - 11 and 16 of the FTRA, an SFI must:

(a) where applicable, obtain senior management approval before establishing new correspondent and other similar relationships and a review of these relationships should be conducted at least annually;

(b) identify and verify the identity of the respondent institution with which they enter into a correspondent relationship;

(c) collect sufficient information on the respondent institution to fully understand the nature of its business and activities and determine from publicly available information the reputation of the respondent and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;

(d) evaluate the controls implemented by the respondent institution with respect to identified risks, and establish an agreement on the respective responsibilities of each party under the relationship, with particular regard to the rigor of the respondent institution's controls;

(e) in the case of a trust, an implied trust or other legal arrangement resulting in the severance of legal ownership from beneficial interest by means of a legal device or entity, be satisfied that the beneficial owner has been appropriately identified; and

(f) in the case of a payable-through account, satisfy itself that the respondent institution —

- has conducted customer due diligence on the facility holder that have access to the account;
- has implemented mechanisms for on-going monitoring with respect to the facility holder; and
- is able to provide relevant customer due diligence information to the financial institution upon request.

The above requirements are outlined in section 10 of the FTRA.

175 SFIs must not maintain relationships with banks that have no physical presence[1] in any country or with respondent financial institutions that permit their accounts to be used by such banks.

176 SFIs should terminate, with reasonable notice, the accounts of respondents who fail to provide satisfactory answers to reasonable enquiries including, where appropriate, confirming the identity of customers involved in unusual or suspicious transactions.

C. Politically Exposed Persons ("PEPs")

177 The definition of a politically exposed person is taken from the FTRA, 2018. The other definitions in this paragraph are drawn from the FATF Recommendations.

For the purposes of this section -

"close associate" means a natural person who is closely connected to a PEP, either socially or professionally, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the PEP;

"family member" includes a parent, child, spouse and sibling of the politically exposed person;

"international organisation" means an entity established by formal political agreements between member countries that have the status of international treaties, whose existence is recognised by law in member countries and which is not treated as a resident institutional unit of the country in which it is located;

"politically exposed person" means an individual who is or has been entrusted with -

(a) a domestic prominent public function, inclusive of a head of state or government, legislator, politician, senior government, judicial or military official, senior executive of a state-owned corporation, or important political party official;

(b) a prominent public function by a foreign jurisdiction, inclusive of, a head of state or government, legislator, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation, or senior political party official; or

(c) a senior position at an international organisation or branch thereof, domestic or foreign, and includes a family member or close associate of a politically exposed person; and

"prominent public functions" includes the roles held by a head of state, a head of government, senior officials in the executive, legislative, administrative, military or judicial branches of a government (whether elected or not), senior officials of major political parties, senior executives of government-owned corporations and senior management of international organisations e.g. director, deputy directors and members of the board or equivalent functions, but shall not include middle ranking or more junior officials.

The requirements set out in this section are applicable to family members and close associates of all types of PEPs.

For further guidance, see Appendix C for a list of websites with relevant information.

178 SFIs are encouraged to be vigilant in relation to PEPs from all jurisdictions, in particular High-Risk Countries (see paragraphs 185 and 186), who are seeking to establish business relationships. In relation to all PEPs, in addition to performing normal due diligence measures, SFIs must, using a risk-based approach, perform the following enhanced CDD measures:

(i) deploy appropriate risk management systems to determine whether the customer or a beneficial owner of the customer is a PEP;

(ii) develop a clear policy and internal guidelines, procedures and controls regarding such business relationships;

(iii) obtain senior management approval for the commencement of business relationships with such customers or to continue business relationships with customers who are found to be or who subsequently become PEPs;

(iv) take reasonable measures to establish the source of wealth and source of funds of the customer and the beneficial owner of the customer; and

(v) conduct enhanced monitoring of the business relations with and transactions for the customer, so that any changes are detected and

consideration can be given as to whether such changes appear unusual or suspicious.

179 SFIs should also adopt a risk-based approach in determining whether to perform the enhanced CDD measures as set out in paragraphs 177 (ii) through (iv) and 181 or the extent of enhanced CDD measures to be performed for –

a. domestic politically exposed persons;

b. international organisation politically exposed persons; or

c. politically exposed persons who have stepped down from their prominent public functions, taking into consideration the level of influence such persons may continue to exercise after stepping down from their prominent public functions, except in cases where their business relations or transactions with the SFI present a higher risk for money laundering or terrorism financing.

180 SFIs should ensure that timely reports are made to the FIU where proposed or existing business relationships with PEPs give grounds for suspicion.

181 SFIs should develop and maintain "enhanced scrutiny" practices which may include the following measures, to address PEP risks:

(i) SFIs should assess country risks where they have financial relationships, evaluating, *inter alia*, the potential risk for corruption in political and governmental organizations. (See the sources set out in Appendix C). SFIs which are part of an international group might also use the group network as another source of information;

(ii) where SFIs consider business relations with entities and nationals of countries vulnerable to corruption, they should establish who the senior political figures are in that country, and should also seek to determine, whether or not their customer has close links with such individuals (for example immediate family or close associates). SFIs should note the risk that customer relationships may be susceptible to acquiring such connections after the business relationship has been established; and

(iii) SFIs should be vigilant where their customers are involved in those businesses which appear to be most vulnerable to corruption, including, but not limited to trading or dealing in precious stones or precious metals.

182 In particular, detailed due diligence should include:

(i) close scrutiny of any complex structures (for example, involving legal structures such as corporate entities, trusts, foundations, executive entities

and any other legal arrangements for the purposes of transparency, and identifying the beneficial ownership and/or the exercise of ultimate effective control over the assets);

(ii) every effort to establish the source of wealth (including the economic activity that created the wealth) as well as the source of funds involved in the relationship, both at the outset of the relationship and on an ongoing basis;

(iii) the development of a profile of expected activity on the business relationship so as to provide a basis for future monitoring. The profile should be regularly reviewed and updated;

(iv) a review at senior management or board level of the decision to commence or continue the business relationship and regular review, on at least an annual basis, of the development of the relationship; and

(v) close scrutiny of any unusual features, such as very large transactions, the use of government or central bank accounts, particular demands for secrecy, the use of cash or bearer bonds or other instruments which break an audit trail, the use of unknown financial institutions and regular transactions involving sums just below a typical reporting level.

183 There should be full documentation of the information collected in line with SFIs' policies to avoid or close business relationships with PEPs. If the risks are understood and properly addressed then the acceptance of such persons becomes a business/commercial decision as with all other types of customers. SFIs should refer to Appendix C for a list of websites relevant to the risks associated with PEPs.

D. High-Risk Countries Under Increased Monitoring

184 Certain countries are associated with predicate crimes such as drug trafficking, fraud and corruption and with terrorist financing, proliferation financing and consequently pose a higher potential risk to SFIs. Engaging in business relationships with customers who are either citizens of, or domiciled, in such countries exposes the SFI to reputational, compliance and legal risk. SFIs are encouraged to consult publicly available information sources including the FATF list of High-Risk jurisdictions subject to Call for Action and Jurisdictions under Increased Monitoring [12] to ensure that they are aware of countries/territories identified as having strategic deficiencies in their

[12] Financial Action Task Force (FATF), "High-Risk Jurisdictions subject to a Call for Action and Jurisdictions under Increased Monitoring," available at: https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html

AML/CFT/CPF systems and which may pose a higher risk. SFIs should refer to Appendix C for a list of relevant websites.

185 Caution should also be exercised in respect of the acceptance of certified documentation from individuals and entities located in high-risk countries and territories. SFIs should perform enhanced verification checks on such individuals/entities to ensure the legitimacy and reliability of the documentation and the underlying customer relationship.

E. Bearer Shares

186 Pursuant to section 196 (3) of the International Business Companies Act, (IBC 2000) bearer shares are not permitted in The Bahamas.

Bearer shares pose a material AML/CFT/CPF risk due to inherent anonymity and potential for abuse. In evaluating the risk associated with a given customer relationship, the SFI must determine whether any legal person customer, beneficial owner, or ultimate principal has issued or has the potential to issue bearer shares. Bearer shares, by their nature, enable the holder to exercise ownership rights without an identifiable registered holder, creating opportunities for concealment of beneficiaries and proceeds of crime.

Accordingly, SFIs shall not accept, recognize or rely upon bearer shares or bearer share instruments. The existence, presentation or attempted use of bearer shares shall be treated as a high-risk indicator requiring immediate enhanced due diligence and appropriate risk-mitigation measures.

187 Contravention of this Section, or - non-compliance with the ongoing obligations may attract administrative monetary penalties, and/or and other sanctions as determined appropriate by the Central Bank.

TREATMENT OF PREVIOUS BUSINESS RELATIONSHIPS

188 Prior to its re-enactment, the FTRA required that SFIs verify the identity of customers with facilities established prior to 29th December, 2000 (‘‘existing facilities”). Where a SFI had not verified the identity of any such customer by a previously specified date, the SFI was required to notify the Central Bank. SFIs should have regard to the paragraphs which follow when dealing with existing customers.

189 Any customer that has not been properly identified and risk rated presents a threat of money laundering, terrorist financing, or other identified risks.

190 In light of the above, the Central Bank has a supervisory expectation that SFIs will implement appropriate measures to satisfy the verification requirements outlined in these Guidelines, or take steps to suspend or terminate the business relationship.

191 SFIs are also reminded of the suspicious transaction reporting duties imposed by the FTRA (see section 7, 11, 25 - 30, and 49 - 50). Where a customer refuses to provide the information necessary for his identity to be verified, this raises questions about the reasons for non-cooperation and whether the business relationship is being used in connection with any identified risk activity.

192 Where persons lack standard identification documents, some flexibility is suggested as outlined in Section A3 above. For existing customers, an introduction from a respected customer personally known to a Director, Manager or senior member of staff, will often provide some comfort, as long as the guidance outlined in Section A3 is followed. The introduction cannot replace the verification procedures described in these Guidelines; SFIs must keep details about who initiated the account and authorized the introduction. Directors/Senior Managers should take a common-sense approach in determining whether certain documents should be waived. Where specific customer documentation is waived, management must document why the waiver was granted.

193 When an existing customer closes one account and opens another, or enters into a new agreement to purchase products or services, there is no need to re-verify identity. However, it is an opportune time to confirm the relevant customer information. This is particularly important when a previously non-active account has been reactivated, or there has been no recent contact/correspondence with the customer (e.g. within the last twelve months).

ON-GOING MONITORING OF BUSINESS RELATIONSHIPS

194 Once the identification procedures have been completed and the client relationship is established, SFIs should monitor the conduct of the relationship/account to ensure that it is consistent with the nature of business stated when the relationship/account was opened.

Monitoring

195 SFIs are expected to implement systems and controls to monitor relevant account activities on an ongoing basis. The nature of this monitoring will depend on the nature of the business. Higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring. This monitoring will allow SFIs to be vigilant, and note any significant changes or transactions which are inconsistent with the original stated purpose of the account(s). Some possible areas to monitor are:

(a) transaction type;
(b) frequency;
(c) amount;
(d) geographical origin/destination; and
(e) account signatories.

196 When establishing and maintaining relationships with cash-intensive businesses, SFIs should establish policies, procedures, and processes to identify high-risk relationships; assess AML/CFT/CPF risks; complete due diligence at account opening and periodically throughout the relationship; and include such relationships in appropriate monitoring for unusual or suspicious activity.

197 Depending on the type of business a SFI conducts and the nature of its client portfolio, each SFI may wish to set its own parameters for the identification and further investigation of cash transactions. For those customers deemed to be particularly high risk, SFIs should implement enhanced practices, such as periodic on-site visits, interviews with the business's management, or closer reviews of transactional activity.

198 The most effective method of monitoring of accounts/business relationship is achieved through a combination of computerised and manual solutions. A corporate compliance culture, and properly trained, vigilant staff will form an effective monitoring method as a matter of course. Computerised approaches may include the setting of "floor levels" for monitoring by amount.

199 SFIs should invest in computer systems specifically designed to assist the detection of money laundering and other crimes. It is recognized however that this may not be a practical option for some SFIs due to cost, the nature of their business, or difficulties of systems integration. In such circumstances SFIs should ensure they have comparable alternative systems in place, which provide sufficient controls and monitoring capability for the timely detection and reporting of suspicious activity.

"Hold Mail" Accounts

200 "Hold Mail" accounts are accounts where the accountholder has instructed the SFI not to issue any correspondence to the accountholder's address.

201 Regardless of the source of "Hold Mail" business, evidence of identity of the account holder should be obtained by the SFI in accordance with Appendix B and paragraphs 61 (i) – (iii) and 62 (i) and (ii) of these Guidelines.

202 It is recommended that SFIs have controls in place for when existing accounts become "Hold Mail" accounts, and that the necessary steps to obtain the identity of the account holder are taken (where such evidence is not already on the SFI's file).

203 Accounts with a "c/o" address should not be treated as "Hold Mail" accounts, as mail is being issued, albeit not necessarily to the account holder's address. There are many genuinely innocent circumstances where a "c/o" address is used, but SFIs should monitor such accounts more closely as these accounts may represent additional risk.

204 Hold Mail" accounts should be annually monitored and reviewed. SFIs should establish procedures to conduct annual checks of the valid contact details of hold mail customers.

V MONEY TRANSMISSION BUSINESSES

205 The following guidance applies to persons other than banks, credit unions or trust companies licensed under the BTCRA:

"Money transmission business" ("MTB") is as defined in section 2 of the BTCRA (as amended), namely, the business of accepting cash, cheques, other monetary instruments or other stores of value in one location and the payment of a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the money transfer business belongs. Remittances may be domestic or international.

a " Money transmission service provider" is defined as any person carrying on a money transmission business.

a "Money transmission agent" is defined as any person carrying on money transmission business on behalf of a money transmission service provider.

206 In accordance with section 3(1)(h)(v) of the FTRA, providers and their agents are covered by the definition of "financial institutions". Consequently,

providers and their agents are required to adhere to all of the requirements of the FTRA, the FTRR, the FIUA and subsidiary legislation made thereunder.

207 Each MTB must have an AML/CFT/CPF programme in place comprising policies to prevent money laundering, terrorist financing, and other identified risks. Such policies should include provisions for:-

(a) the internal systems of controls, policies and procedures;
(b) customer due diligence procedures;
(c) a risk-based framework;
(d) a records management system; and
(e) education and training of employees and money transmission agents in recognising and reporting suspicious transactions.

A MTB must:–

- include its money transmission agents in its AML/CFT/CPF programme;
- monitor its money transmission agents for compliance with its AML/CFT/CPF programme; and
- document the basis on which it is satisfied with its money transmission agents' compliance with the AML/CFT/CPF programme.

Where a MTB observes any non-compliance with its AML/CFT/CPF programme, it should document its findings and consider remedial action, such as termination of the agency agreement. The MTB should obtain approval from its senior management on the proposed action to be taken, including any "no-action" proposal.

Vulnerability of MTBs to Money Laundering & Terrorist Financing

208 Most MTBs have a fleeting relationship with their customers, making them vulnerable to money laundering and the financing of terrorism. Whereas a person would typically have to be a customer with an account at a bank, for example, to be able to access the services of that bank, a person does not have that type of relationship with the MTB and can use different MTBs to transact business. The MTB is particularly vulnerable due to the high volume of cash handled on a daily basis and the ability to transmit funds instantly to any part of the globe.

209 While the international remittance system is typically used by expatriate workers to send some of their earnings back home, it can also be used to transmit the proceeds of criminal activities and funds used to finance terrorism. The rapid movement of funds across multiple jurisdictions presents a challenge to investigators, particularly if the identity of the originator is unclear. For this reason, international standards have been developed with respect to payer

information (see Section VI of these Guidelines) that should accompany wire transfers to mitigate the abovementioned risk.

210 Apart from money transmission, cheque cashing is another important segment of the business for some MTBs. MTBs should be aware that endorsed third party cheques from overseas are a money laundering risk. Even where a Bahamian dollar cheque, endorsed by a third party, is presented to the MTB for cashing, the MTB should take appropriate steps to ascertain the economic purpose behind the endorsement to that person presenting the cheque. Large cheques originating from unknown individuals present a greater money laundering risk compared to small cheques originating from well-established businesses.

Identification Documentation

211 Proper identification documentation is required for **all** money transmissions. The requirement for specific pieces of payer information that are to accompany each wire transfer applies to money transmissions. MTBs must therefore request and obtain identification documentation for money transmissions, in line with the payer information requirements in Section VI "Electronic Funds Transfers" set out below.

Customer identification information must be obtained **prior** to a transaction being carried out. If identification information is not obtained, the transaction should not proceed.

For further guidance on customer identification and record keeping requirements, MTBs should refer to Sections IV and VII of these Guidelines.

Transaction Monitoring

212 Because of the large number of customers involved and the relatively small amounts transacted, it is imperative for MTBs to have adequate systems in place to collate relevant information and monitor customers' activities. In the MTB, the amount of information collected may be broadened to include details of the recipient of the funds. This information will assist MTBs to determine whether there is any risk that the customer is utilising multiple recipients to facilitate money laundering or whether multiple customers are remitting multiple small sums that are accumulated with one recipient.

Indicators of the Misuse of MTBs

213 The following activity may be suspicious and indicate money laundering or other illegal activity through the misuse of MTBs.

Transactions Which Do Not Make Economic Sense

- Transactions which are incompatible with the SFI's knowledge and experience of the customer in question, or with the purpose of the relevant business transaction.

- A customer or group of customers attempt to hide the size of a large cash transaction by breaking it into multiple, smaller transactions. For example, the smaller transactions may be conducted -

    1. at different times on the same day;
    2. with different MTB cashiers on the same day or different days; and
    3. at different branches/offices of the same MTB.

- Transactions that cannot be reconciled with the customer's usual activities.
- A business customer sends or receives money transfers to/from persons in other countries with no apparent business reason. Or, they give a reason inconsistent with their business.
- A business customer sends or receives money transfers to or from persons in other countries when the nature of their business would not normally involve international transfers.

Transactions Involving Large Amounts of Cash

- Frequent transactions of large cash amounts that do not appear to be justified by the customer's business activity.
- Large and regular payments that cannot be identified as bona fide transactions, to countries associated with the production, processing or marketing of narcotics or other illegal drugs.
- Cash payments remitted to a single account by a large number of different persons without an adequate explanation.

Other Types of Transactions and Activity

- Transaction volume and activity is not commensurate with the customer's known profile (e.g. age, occupation, income).
- Transactions with countries or entities that are reported to be associated with terrorist activities or with persons that have been designated as terrorists.
- Use of multiple transactions and multiple recipients, including structuring of transactions to avoid an identification threshold of $1,000 or whatever enhanced due diligence threshold that the MTB may have.

- A business customer that is reluctant to provide complete information regarding: the type of business, the purpose of the transaction, or any other information requested by the MTB.

VI ELECTRONIC FUNDS TRANSFERS

214 The Financial Action Task Force ("FATF"), an inter-governmental, standard setting body that issues international standards to guide governments in their implementation of measures to combat money laundering associated with organized crime, terrorism financing and, more recently, the proliferation of weapons of mass destruction, updated those international standards in 2012. The FATF's Recommendation 16 (formerly Special Recommendation VII) is aimed at enhancing the transparency of cross-border and domestic electronic funds transfers ("wire transfers" or "transfers") thereby making it easier for law enforcement to trace funds transferred electronically by terrorists and other criminals. Recommendation 16 has been implemented in The Bahamas through the Financial Transactions Reporting (Wire Transfers) Regulations, 2018 ("the Wire Transfers Regulations").

214.1 The Wire Transfers Regulations are intended to cover any transaction carried out on behalf of a payer through a financial institution by electronic means with a view to making funds available to a payee at a beneficiary financial institution, whether or not the payer and the payee are the same person. Wire transfers consists of all forms of electronic transmissions including, but not limited to, email, facsimile, short message service or other means of electronic transmission for payment instructions. Generally, the Wire Transfers Regulations require financial institutions that participate in the execution of wire transfers to obtain, record and retain specified information on payers and payees of wire transfers and to ensure that all transfers are accompanied throughout the payment chain by information on the payers who give the instructions for payment to be made and the payees who receive the transferred funds.

Pre-conditions for Making Funds Transfers - Verification of Identity of Payers

214.2 SFIs that initiate wire transfers on behalf of payers (referred to as "originating financial institutions") must ensure that the payer information conveyed in the payment message or instruction is accurate and has been verified.

214.3 The verification requirement is deemed to be met for account holding customers of the originating financial institution once the customer's identity has been verified and the verification documentation has been retained in accordance with the FTRA and the FTRR. In such cases, the originating financial institution may assign to the wire transfer a unique transaction identifier that would link the account holding customer and his relevant identification information to the wire transfer.

214.4 Before initiating one-off wire transfers on the instructions of non-account holding customers, originating financial institutions must verify the payer's identity and address (or a permitted alternative to the payer's address – i.e. the payer's date and place of birth or the payer's national identity number).

Monitoring Wire Transfers for Sanctioned Persons, Entities or Countries/Jurisdictions

214.4.1 SFIs that participate in the execution of wire transfers should monitor wire transfers to and from higher risk countries or jurisdictions under increased monitoring, as well as transactions with higher risk countries or jurisdictions. Wire transfers or transactions with sanctioned parties or countries or jurisdictions listed in Orders issued pursuant to the International Obligations (Economic and Ancillary Measures) Act, 1993 should suspended or rejected.

214.4.2Where name screening checks confirm that a wire transfer's payer and or payee is a terrorist or terrorist entity, the requirement for the SFI to reject or suspend wire transfers of these terrorists or terrorist entities cannot be risk-based.

214.4.3 Where there are positive hits arising from name screening checks, they should be escalated to the MLRO and reported to the Financial Intelligence Unit and the Central Bank. The decision to approve or reject the receipt or release of the wire transfer or to suspend the wire transfer should be made at an appropriate level (for example, by the Compliance Officer or a senior manager) and should be clearly documented.

SFIs should also apply the procedures and reporting requirements set out in the *GFSR Guidance Notes on Targeted Financial Sanctions Reporting Forms* (June 2025) [13] when completing and submitting any targeted financial sanctions reports.

Cross-border Wire Transfers of Below $1,000 - Reduced Payer Information

214.5 Originating financial institutions may apply simplified due diligence for cross-border wire transfers below $1,000 provided that such transfers are considered

[13] GFSR, *Guidance Notes on Targeted Financial Sanctions Reporting Forms*, 27 June 2025 (Group of Financial Services Regulators of The Bahamas), https://www.centralbankbahamas.com/viewPDF/documents/2025-06-27-09-47-59-GFSR-GUIDANCE-NOTES-ON-TARGETED-FINANCIAL-SANCTIONS-REPORTING-FORMS.pdf

to present a low risk of money laundering or terrorist financing. The minimum information required to accompany these wire transfers is –

(i) the payers name and account number, where such account is used to process the transaction or, if no account is used, a unique transaction identifier; and

(ii) the payee's name and account number, where such account is used to process the transaction or, if no account is used, a unique transaction identifier.

Cross-border Wire Transfers of $1,000 or More - Complete Payer and Payee Information

214.6 Except as permitted below, complete payer and payee information must accompany all wire transfers of $1,000 or more where the beneficiary financial institution (i.e. the financial institution that receives a funds transfer on behalf of a payee) is located in a jurisdiction outside The Bahamas. Complete payer information includes the information set out in sub-paragraph 214.5 (i) as well as the payer's address, or date and place of birth, or the payer's national identity number, or customer identification number. Complete payee information is as indicated in sub-paragraph 214.5 (ii).

214.7 The extent of the information supplied in each field of the payments message will be subject to the conventions of the messaging system used and is not prescribed in detail in the Wire Transfers Regulations. For example, where the wire transfer is debited from a joint account, while it is preferable to provide all of the joint account holders' information to the beneficiary institution, the originating financial institution may demonstrate that it has met its legal obligation to provide a payer's name where, dependent upon the size of the field, it provides the name of one or more account holders.

214.8 Where the wire transfer is not debited to a bank account, the requirement for an account number must be substituted by a unique transaction identifier which permits the transfer to be traced back to the payer. The Wire Transfers Regulations define "unique transaction identifier" as "a combination of letters, numbers, or symbols, determined by a financial institution in accordance with protocols of the payment and settlement system, or messaging system, used to effect the transfer of funds, which permits traceability of the transaction to the payer and the payee".

214.9 Only the address of a payer may be substituted with the payer's date and place of birth, or national identity number or customer identification number. A national identity number (such as an identity card number, birth certificate number, or passport number or, where the wire transfer originator is not a natural person, the incorporation number or business registration number) may be a

number contained in an official document. A customer identification number may be an internal reference number that is created by the originating financial institution which identifies a payer, and which will continue throughout a business relationship.

214.10 Payers should be provided with an opportunity to request substitute information for an address on transfers. It follows that in the event a beneficiary financial institution (i.e., a financial institution that receives funds on behalf of a payee) demands the payer's address, where one of the alternatives had initially been provided, the response to the enquiry should point that out. Only with the payer's consent or under judicial compulsion should the address be additionally provided.

214.11 In order to ensure that the information required under the Wire Transfers Regulations is also processed in line with the Data Protection (Privacy of Personal Information) Act, 2003 ("the DPA"), originating financial institutions must have regard to the fair processing requirements of the DPA and ensure that its terms and conditions of business (or other communication) with each payer include reference to the information that may accompany wire transfers.

Domestic Wire Transfers - Reduced Payer Information

214.12 Where the originating and beneficiary financial institutions are both located within The Bahamas, wire transfers need be accompanied by the reduced information set out in paragraph 214.5. However, if requested by the beneficiary financial institution, complete payer information must be provided by the originating financial institution within three business days of such request.

Batch File Transfers

214.13 A batch file transfer contains several individual transfers from a single payer bundled together for transmission to one or more beneficiaries outside The Bahamas. For batch file transfers of $1,000 or more, a hybrid complete/reduced payer and payee information requirement applies. Individual transfers within the batch file need carry only the payer's account number or, if no account is used, a unique transaction identifier. However, the batch file itself must contain complete payer and payee information.

Wire Transfers via Intermediaries

214.14 Intermediary financial institutions are SFIs, other than originating or beneficiary financial institutions that participate in the execution of wire transfers. Intermediary financial institutions must take reasonable measures to identify wire transfers that lack the required payer and payee information. In addition, intermediary financial institutions should, subject to the following guidance on technical limitations, ensure that all information received on the payer and payee

which accompanies a wire transfer is retained with the transfer throughout the payment chain.

Technical Limitations

214.15 It is preferable for payments to be forwarded through a system which is capable of carrying all the required payer and payee information. However, where an intermediary financial institution is technically unable to transmit complete payer and payee information, it may nevertheless use a system with technical limitations provided that:

(a) if it is aware that the payer and or payee information is missing or incomplete, it must concurrently advise the beneficiary financial institution or another intermediary financial institution of that fact by an agreed form of communication, whether within a payment or messaging system or otherwise; and

(b) it retains records of any payer and payee information received with the wire transfer for five years from receipt of the information, whether or not the information is complete. If requested to do so by the beneficiary financial institution or another intermediary financial institution, the intermediary financial institution must provide the payer and or payee information received with the wire transfer within three business days of receiving the request.

Duty to Assess Risks

214.16 As part of their internal controls, intermediary financial institutions must adopt risk-based procedures that enable them to determine when to execute, reject, or suspend wire transfers that are not accompanied by the required payer and payee information. The procedures should also outline the appropriate follow-up action to take in these cases.

Minimum Standards

214.17 The above information requirements are minimum standards. It is open to SFIs to elect to supply complete payer information with transfers which are eligible for a reduced information requirement where systems permit, thereby limiting the likely incidence of inbound requests for complete information. To ensure that the data protection position is beyond any doubt, it would be advisable to ensure that terms and conditions of business include reference to the information being provided.

Record Keeping Requirements

214.18 The particulars of the wire transfer to be recorded must be of sufficient detail so

as to enable the transfer to be accurately described. This information, together with information on the payer and payee (including the payer's identity verification documentation) must be retained by the originating financial institution for a period of five years from execution of the transfer.

Beneficiary Financial Institutions - Checking Incoming Wire Transfers

214.19 The Wire Transfers Regulations specify that beneficiary financial institutions should adopt risk-based procedures to detect whether required payer and payee information is missing from wire transfers received by them and to determine whether the absence of required information should give rise to a suspicious transaction report being made to the FIU.

214.20 In practical terms, it is expected that payer and payee information requirements will be met by a combination of the following:

(a) SWIFT payments on which mandatory payer and payee information fields are not completed will fail to process and the payment will not be received by the beneficiary financial institution. Current SWIFT validation prevents payments being received where the mandatory information is not present at all. However, it is accepted that where the payer information fields are completed with incorrect or meaningless information, or where there is no account number, the payment will pass through the system.

(b) beneficiary financial institutions should therefore subject incoming wire transfers to an appropriate level of post event random sampling to detect noncompliant payments. This sampling should be risk based. For example:

(i) the sampling could normally be restricted to payments emanating from originating financial institutions outside The Bahamas where the complete payer information requirement applies;

(ii) the sampling could be weighted towards those jurisdictions deemed high risk under SFIs' own country risk rating;

(iii) the sampling could be focused more heavily on transfers from those originating financial institutions who are identified by such sampling as having previously failed to comply with the relevant information requirement;

(iv) other specific measures might be considered, for example, checking, at the point of payment delivery, that payer information is compliant and meaningful on all transfers that are collected in cash by payees

on a ―pay on application and identification basis. It should be noted that none of the above requirements obviate the obligation to report suspicious transactions.

If a beneficiary financial institution becomes aware in the course of processing a payment that it contains meaningless or incomplete information, it should either reject the transfer or ask for complete payer information.

214.21 Where an originating financial institution is identified as having regularly failed to comply with the payer and payee information requirements, the beneficiary financial institution should give the originating financial institution a reasonable time within which to correct its failures. Where the originating financial institution, after being given a reasonable time within which to do so, fails to provide the missing information, the beneficiary financial institution should either refuse to accept further transfers from that originating financial institution or decide whether to terminate or restrict its business relationship with that originating financial institution. The beneficiary financial institution must advise the Central Bank of any decision to reject future transfers, or to terminate or restrict its relationship with the non-compliant originating financial institution within ten (10) business days of such decision being taken.

214.22 It should be borne in mind when querying incomplete payments that some countries, like The Bahamas, may have framed their own regulations to incorporate a threshold of $1,000, below which the provision of complete payer information on outgoing payments is not required. However, this does not preclude beneficiary financial institutions from calling for the complete payer information where it has not been provided, but it is reasonable for a risk-based view to be taken on whether or how far to press the point.

Exemptions

214.23 The Wire Transfers Regulations specifically exempt the following payment types:

(a) transfers where the payer withdraws cash from his or her own account;

(b) transfers by credit or debit card so long as the payee has an agreement with the financial institution permitting payment for goods or services and a unique identifier, allowing the payment to be traced back to the payer, accompanies all transfers;

(c) direct debits from accounts authorized between two parties so long as a unique identifier, allowing the payment to be traced back to the payer, accompanies all transfers;

(d) transfers to public authorities for the payment of fines, penalties, duties or other taxes within The Bahamas; and

(e) transfers where both the payer and payee are financial institutions acting on their own behalf.

Card Transactions

214.24 As indicated in paragraph 214.23 (b), credit or debit card transactions for goods and services are out of the scope of the Wire Transfers Regulations provided that a unique identifier, allowing the transaction to be traced back to the payer, accompanies the movement of the funds. The 16 digit Card PAN number serves this function.

214.25 Complete payer information is required in all cases where the card is used to generate a direct credit transfer, including a balance transfer, to a payee's beneficiary financial institution located outside The Bahamas.

Offences and Fines

214.26 Financial institutions that fail to comply with the provisions of the Wire Transfers Regulations commit an offence and are liable upon summary conviction to a fine of two hundred thousand dollars. As an alternative to prosecution, the Central Bank may impose a fine of the same amount. SFIs are also reminded of the Central Bank's power to impose administrative penalties of up to $200,000 for a company or up to $50,000 for an employee, director or senior manager of a SFI where these persons contravene the provisions of the Wire Transfers Regulations (see earlier section of these Guidelines on Penalties For Non-Compliance).

VII - RECORD KEEPING

215 Sections 15, 16 and 17 of the FTRA require financial institutions to retain records concerning customer identification and transactions for use as evidence in any investigation into money laundering, terrorist financing or proliferation financing. This is an essential component of the audit trail procedures. If the FIU and law enforcement agencies investigating a money laundering or terrorist financing case cannot link criminal funds passing through the financial system with the original criminal money generating such funds, then confiscation of the criminal funds cannot be effected.

Sometimes the only significant role a SFI can play in a money laundering, terrorist financing or proliferation financing investigation is through the provision of relevant records, particularly where the money launderer, terrorist

financier or proliferation financier has used a complex web of transactions specifically for the purpose of confusing the audit trail.

The statutory requirements detailed in the following paragraphs are designed to ensure, in so far as is practicable, that a SFI can provide the authorities with its section of the audit trail in any subsequent investigation.

216 The records prepared and maintained by a SFI on its customer relationships and transactions should be such that:

- requirements of legislation are fully met; competent third parties will be able to assess the SFI's observance of AML/CFT/CPF policies and procedures;
- any transactions effected via the SFI can be reconstructed;
- and the SFI can satisfy court orders or enquiries from the appropriate authorities.

Verification of Identity and Other Records

217 For the purpose of verifying the identity of any person, SFIs must keep such records as are reasonably necessary to enable the nature of the evidence used for the purposes of that verification to be readily identified by the FIU.

218 Records relating to the verification of the identity of facility holders and beneficial owners, account files and business correspondence, and results of any analysis undertaken must be retained for at least five years from the date a person ceases to be a facility holder.

219 In keeping with best practices, the date when a person ceases to be a facility holder is the date of:

(i) the carrying out of a one-off transaction or the last in the series of transactions; or
(ii) the ending of the business relationship, i.e., the closing of the account or accounts.

220 Where formalities to end a business relationship have not been undertaken, but a period of five years has elapsed since the date when the last transaction was carried out, then the five-year retention period commences on the date of the completion of the last transaction, investigation, or prosecution of any offence.

Format of Records

221 SFIs should have standard procedures which seek to reduce the volume and density of records which must be stored, whilst still complying with statutory requirements. The FTRA requires that where records are not kept in written

form, they must be kept in a form readily accessible and convertible to written form. Retention may, therefore, be by way of original documents, stored on microfiche, computer disk or in other electronic form.

222 SFIs which store original documents in a computerized form should have regard to the requirements of the Evidence Act, 1996 as regards the admissibility of documents via computerised evidence or the production of evidence of records in written form as well as those kept on microfilm or any other form of mechanical or electronic data retrieval mechanism.

VIII - THE ROLE OF THE MONEY LAUNDERING REPORTING OFFICER

223 SFIs should appoint a MLRO to whom employees must report their knowledge or suspicions of customers who are engaged in money laundering, terrorist financing or proliferation financing.

224 The type of person appointed as MLRO will depend upon the size, structure and nature of the SFIs business, however, he or she should be of sufficient seniority and possess the authority to discharge the responsibilities of the role effectively.

225 The MLRO has significant responsibilities and is required to determine whether the information or other matters contained in the transaction report received gives rise to a knowledge or suspicion that a customer is engaged in money laundering, terrorist financing or proliferation financing.

226 In making this judgment, the MLRO should have timely access to all other relevant information available within a SFI concerning the person or business to which the initial report relates (such as customer identification data, other CDD information and transaction records). This may include a review of other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship, and reference to identification records held. If, after completing this review, the MLRO determines that the initial report gives rise to a knowledge or suspicion of money laundering, terrorist financing or proliferation financing, then the MLRO must disclose the information relating to money laundering to the FIU and terrorist financing and proliferation financing to the Commissioner of Police.

227 The "determination" by the MLRO implies a process with at least some formality attached to it. For the MLRO's own protection, it would be prudent for internal procedures to require that only written reports of suspicious transactions are submitted to the MLRO, who should record his or her determination and the underlying reasons in writing.

228 The MLRO will be expected to act honestly, reasonably and to make determinations in good faith.

IX – EDUCATION AND TRAINING REQUIREMENTS

229 SFIs must implement ongoing training programmes to ensure employees maintain awareness of:

- all AML/CFT/CPF policies and procedures, including those for identification, record keeping, the recognition and handling of unusual and suspicious transactions and internal reporting; and
- any applicable AML/CFT/CPF legislation.

The Need for Staff Awareness

230 The effectiveness of the procedures and recommendations contained in these Guidelines depend on the extent to which staff of financial institutions appreciate the serious nature of the background against which these Guidelines have been issued. Staff must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All staff should be encouraged to co-operate fully and to provide a prompt report of any unusual or suspicious transactions without fear of reprisal.

231 It is mandatory that organisations conducting banking, trust and money transmission activities covered by these Guidelines introduce comprehensive measures to ensure that staff are fully aware of their responsibilities.

Identifying Suspicion

232 The types of transactions which may be used by money launderers are almost unlimited. As a result, it can be difficult to define a suspicious transaction. However, it is important to properly differentiate between the terms “unusual” and “suspicious”.

233 A transaction is considered *unusual* when it has no apparent economic, or visible lawful purpose, or the amount, origin, destination, or transaction type is inconsistent with a client’s known legitimate business or personal activities. SFIs should investigate the background and purpose of such transactions, as far as is reasonably practicable, and document their findings.

234 Where SFIs observe unusual activity in relation to any client account, they should question the customer concerned, even if it means asking difficult

questions. If a customer fails to provide credible answers, this should invite further enquiry about his activities, make the SFI reconsider the wisdom of doing business with him and, potentially lead to a STR being filed. SFIs should document the results of their enquiries into unusual activity.

235 Where a staff member's enquiries produce a satisfactory explanation for the unusual transaction (or pattern of transactions), he may conclude that there are no grounds for suspicion, and choose to take no further action. However, where the enquiries conducted by the staff member do not provide a satisfactory explanation of the transaction, he may conclude that there are grounds for *suspicion* requiring the filing of an STR.

236 Under the FTRA, where any person conducts or intends to conduct any transaction by, through, or with a SFI and the SFI knows, suspects or has reasonable grounds to suspect that the transaction or proposed transaction—

- involves the proceeds of criminal conduct as defined
- Proceeds of Crime Act;
- is related to an offence under the Proceeds of Crime Act;
- is an attempt to avoid the enforcement of any provision of the
- Proceeds of Crime Act; or
- is an identified risk,

the SFI must report the transaction or proposed transaction to the FIU as soon as practicable after forming that suspicion (see section 825 of the FTRA).

Reporting Procedures

237 The national reception point for disclosure of suspicious transaction reports is the Financial Intelligence Unit, whose address is 2nd Floor, 31B Annex Building, Poinciana House, East Bay Street, Nassau, The Bahamas.

238 A STR must contain the details specified in the First Schedule of the FTRA; a statement of the grounds on which the SFI holds the suspicion; and be submitted in writing to the FIU through its electronic filing platform; **CaseKonnect.** This platform allows MLROs or Designated Reporting Officers (DROs) to complete, file, and submit all STRs along with relevant supporting documentation to the FIU safely and securely.

239 Notwithstanding the requirements in paragraph 238, although the prescribed form for reporting a suspicious transaction to the FIU is via the CaseKonnect platform, in accordance with section 25 subparagraphs (2) and (3) of the FTRA, 2018 STRs may be forwarded to the FIU by way of facsimile transactions, electronic mail, other similar means of communication. In the case of urgent extenuating circumstances, a STR may be made orally to the FIU. In such a case, the SFI must, as soon as practicable, submit a STR to the

FIU which complies with the requirements established in the FTRA (see section 25 – 30 of the FTRA generally). The relevant contact information for the FIU is as follows: Mailing address: P.O. Box SB50086, Telephone No. (242) 356-9808, Fax No. (242) 322-5551 and email: director.fiu@fiubahamas.bs.

240 SFIs should ensure that all contact between their departments or branches with the FIU and law enforcement agencies is reported to the MLRO so that an informed overview of the situation can be maintained. In addition, the FIU will continue to provide information on request to a disclosing institution in order to establish the current status of a specific investigation. SFIs should refer to the FIU's Suspicious Transactions Reporting Guidelines, 2007 for further guidance on reporting STRs.

Education and Training Programmes

241 Timing and content of training for various sectors of staff will need to be adapted by individual SFIs for their own needs. The Financial Intelligence (Transactions Reporting) Regulations, 2001 provide that, at least once per year, financial institutions must provide relevant employees with appropriate training in the recognition and handling of transactions carried out by persons who may be engaged in money laundering. The following is recommended:

(a) New Employees

General information on the background to money laundering, terrorist financing, proliferation financing and the subsequent need for reporting of any suspicious transactions to the MLRO should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority, within the first month of their employment.

At a minimum, new employees should be informed about the importance placed on the reporting of suspicions by the organisation, that there is a legal requirement to report, and that there is a personal statutory obligation in this respect. They should also be provided with a copy of the written policies and procedures in place in the financial institution for the reporting of suspicious transactions.

(b) Cashiers/Foreign Exchange Operators/Advisory Staff

Members of staff who interact directly with the public are the first point of contact with potential money launderers and their efforts are therefore vital to the organisation's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions

and on the procedures to be adopted when a transaction is deemed to be suspicious.

All front-line staff should know and understand the business policy for dealing with occasional customers, particularly where large cash transactions, money transfers, negotiable instruments, certificates of deposit or letters of credit and other guarantees, etc. are involved. There is a need for extra vigilance in these cases.

The proceeds of crime may not only be paid in, or drawn out, across branch counters. It may be transferred by other means, and branch staff should be trained to recognise this. Staff should be encouraged to take note of credit and debit transactions from other sources, e.g., credit transfers, wire transfers and ATM transactions.

(c) Account/Facility Opening Personnel

Those members of staff responsible for account/facility opening and acceptance of new customers must receive the basic training given to cashiers or tellers (described above). Additional training should be provided in key areas, such as the need to verify a customer's identity, and the SFI's account opening and customer/client verification procedures. They should also be familiar with the SFI's suspicious transaction reporting procedures.

(d) Administration/Operations Supervisors and Managers

Those with responsibility for supervising or managing staff should receive comprehensive, higher-level instruction on all aspects of AML/CFT/CPF procedures. This should include the offences and penalties arising from the POCA and the FTRA for non-reporting and for assisting money launderers; procedures relating to the service of production and restraint orders; internal reporting procedures; the requirements for verification of identity, retention of records, and disclosure of suspicious transaction reports under the FIUA, 2000.

(e) Money Laundering Reporting Officer and Compliance Officer

The MLRO and Compliance Officer will require in-depth training on all aspects of the legislation and internal policies. In addition, the MLRO and Compliance Officer will require extensive initial and on-going instruction on the validation, investigation and reporting of suspicious

transactions, the feedback arrangements, and new trends and patterns of criminal activity.

242 To ensure that staff remember their responsibilities, refresher training must be conducted at least annually.

Fit and Proper Considerations for AML/CFT/CPF

243 The Central Bank strongly expects that all persons subject to its supervision and regulation will exercise the highest standards of probity and competence in discharging their duties relevant to ML/FT/PF risks. Individuals failing to meet these standards are subject to removal and/or exclusion from holding positions as senior officials, directors, or MLROs of SFIs.

Appendix A: Typologies and Methods for Money Laundering, Terrorist Financing and Other Illicit Activity

The term "typologies" refers to the various techniques used to launder money and finance illicit activity. They can vary based on the domestic context and type of financial service provided, but some techniques are quite common. Typologies are valuable sources of information for conducting risk assessments, designing systems and controls, policies and procedures, calibrating on-going monitoring, and providing training to employees. This document aims to raise awareness, and provide a starting point for internal training programs, individual development, and further inquiry.

The examples below are courtesy of The Bahamas FIU. They have been adapted from recent Annual Reports, available online. There are also additional sources of information. For example, the FATF has published numerous typologies reports. Some useful websites are listed in Appendix C.

 # 1 – Online Fraud

Mrs. C informed the FIU that she was a victim of fraud. While on Facebook, a Ms. S contacted her about a job opportunity. Ms. S stated that the job would allow Mrs. C to be a mystery shopper at an online retailer. Mrs. C was not suspicious of the offer because she had submitted several applications online.

Ms. S asked for Ms. C's full name, phone contact and her bank account information. She also requested Mrs. C's maximum daily withdrawal limit ($1,000.00 per day). They had no further contact that day.

Three days later, Ms. S contacted Mrs. C and informed her that she was going to transfer $1,000.00 to her account. Mrs. C was told to keep 10% of the funds as payment. Mrs. C stated that Ms. S instructed her to transfer the funds minus the $100.00 payment to Mr. A in Lagos, Nigeria through a wire transfer company with the same name as her new online "employer".

After Mrs. C sent the funds to Mr. A, she attempted an ATM withdrawal, but was unsuccessful. She went into Local Bank No. 1 and was told that the funds in her account were there by fraudulent means. She was asked to return the funds withdrawn from her account, or be reported to the police. Mrs. C consulted an attorney and reported the matter to the FIU.

A few days later, Local Bank No. 2 made a STR regarding one of their clients. Local Bank No. 2 was contacted by Local Bank No. 1 and informed that one of their clients held fraudulently obtained funds. The scenario also involved a Facebook job solicitation and the same wire transfer company. This time, funds were transferred to London. The matter was reported to the police department for investigation.

Warning indicators:

- Unrealistic job proposal
- Reports of fraudulent transfers
- International fund transfers just below the reporting threshold

 # 2 – Placement – failure to demonstrate source of funds

A credit union client, Mrs. J., owned an electronics store. Her credit union became concerned when Mrs. J opened up twelve (12) fixed deposits accounts totalling BSD $200,000.00 within a six-month period. The credit union tried numerous times to confirm with Mrs. J that the funds were derived from her business. An onsite visit to the electronics store showed that Mrs. J had a very small inventory; too small to explain the recent deposits. Without a satisfactory explanation, the credit union was obligated to file a report with the FIU. The FIU analysed the report, but could not ascertain the origin of the large amount of funds. The matter was sent to the police force for investigation.

Warning indicators:

- Large - scale cash deposits
- Account activity not in keeping with KYC
- Unrealistic wealth compared to client profile
- Evasive stance and actions in response to questioning

 # 3 – Fraud – unusual changes in customer behaviour and transaction types

Z Bank & Trust Limited filed a report with the FIU when one of their clients, Mrs. D, was a victim of fraud.

Mrs. D is the beneficial owner of a company that buys and sells precious metals. For many years, Z Bank & Trust acted on instructions received from her personal assistant, JJ. A month before Z Bank & Trust Limited made the STR, the bank received a letter (believed to be from JJ). The letter stated that Mrs. D had a new assistant--Mr. C.

In a series of emails, it appeared that Mrs. D gave her new assistant permission to correspond directly with the bank, and JJ shared Mr. C's email address. Two days later, the bank received an email from a *slightly* different email address, asking about the status of some payments and the balance on the account. The bank requested a phone contact for Mr. C, which he provided. The bank tried to call Mr. C, but could not contact him via phone. When contacted via email, he stated that he was attending a seminar abroad and was unavailable by phone.

The bank suffered a loss of over $500,000.00 through numerous wire transfer to Asia, Europe, and Africa. The matter was referred to the police for investigation.

Indicators:

- Atypical or uneconomical fund transfer(s) to or from foreign jurisdictions

- Subtle change in email address
- Evasive and defensive responses to questioning

 # 4 - International funds transfer scheme (drug trafficking)

A national FIU detected a scheme involving countries in the Pacific and South American regions. The individuals involved used false names and addresses, which made it difficult to use existing intelligence and identify them as known offenders. The persons travelled extensively but maintained bases in the countries from which the funds originated. They made several international funds transfers through a range of financial institutions, all of which were structured (i.e. intentionally kept below the reporting threshold).

This aroused the suspicions of the bank and, after the bank disclosed the transactions, the suspicion of the national FIU. Following further analysis, the case was passed to the police who initiated an investigation.

The activity continued throughout the following year. The police monitored the international movements of the individuals and their financial transactions. International law enforcement suspected that the individuals involved were probably involved in drug trafficking. During the investigation, the police searched a courier arriving from the country where the FIU was located. The suspect was in possession of US $ 90,000 in bank drafts.

Criminal intelligence analysis allowed the suspected coordinator of the heroin importations to be identified. A search of an airfreight package yielded glass sculptures containing almost sixty kilograms of high-grade heroin.

Warning indicators:

- Use of false identification documents
- Numerous international fund transfers just below reporting threshold

 # 5 – Layering – account activity inconsistent with CDD information

V had a bank account at a bank in Southern Europe. Twice, in rapid succession, he received a large amount of funds into the account by transfers from bank accounts in both a central European and another overseas jurisdiction. The sums he received were disproportionate to his general economic activities. V had a small restaurant in a tourist centre at the coast, but no other known sources of income. When the money arrived, he immediately transferred it to another account at the same bank. The account was in the name of a hotel company: BeachCo. Bank officials found this unusual and decided to report the transactions to the national FIU.

The FIU investigation revealed that around the same time, six other individuals also received large amounts of money, which they immediately transferred to the BeachCo account. Sometimes they accomplished this via transfers through third party accounts. All transfers initiated from accounts in the central European or overseas jurisdiction.

FIU inquiries showed that the money transferred to the individuals in Southern Europe was first transferred from an account in the central European country to an account in the overseas country. It seemed increasingly likely to the investigators that someone was trying to hide the origin of the money destined for the BeachCo account. The FIU learned that T, the major shareholder and manager of BeachCo, was a citizen of an Eastern European country who used multiple false names for his banking activities. T was a prominent member of a large criminal organization, entangled in multiple criminal proceedings for homicide, theft and weapons dealing.

As a result of the investigation, the money in the account of the reporting institution was linked with T's criminal activity. The bank accounts of T, V, and the six other individuals were frozen. Their property and assets were confiscated, and hundreds of thousands of dollars' worth of criminal funds were recovered.

Warning indicators:

- A typical or uneconomical fund transfer to or from foreign jurisdiction
- Account activity atypical for account holder
- A typical or uneconomical fund movement within a single financial institution

 # 6 – Layering – inadequate CDD information

A European FIU received two disclosures from two different banks. M, a foreign national, had presented five cheques to be credited into his newly opened company account. He told the banks the US $1,600,000 originated from his real estate company, which recently completed land sales in an African country. Given the scale of the transactions and lack of supporting data, the bank filed a STR with the FIU.

The FIU investigations established a link to M's father, who was serving a twelve-year prison term in another country for fraud, espionage, corruption and other criminal activities. M's father organised a large-scale fraud which caused the collapse of a foreign bank. When M phoned his bankers to request meetings about additional investments by his company, both institutions quickly contacted the FIU. The FIU contacted the local police, who placed him under surveillance as soon as he re-entered the country. He was subsequently arrested on money laundering charges.

Ultimately, M faced charges of criminal conspiracy, money laundering, and fraud. The foreign authorities informed the FIU that M's father had amassed a small fortune, re-investing the money into real-estate companies and financing enterprises registered in his own name, M's name and the names of other family members. In the course of the investigation, M's house was searched. The police found numerous documents related to financial transactions performed by his father.

Warning indicators:

- New customer attempting large transactions with no supporting rationale
- Inadequate support for source of funds

 # 7 – '419' Fraud via MTB

P was involved in a number of money transfers to West Africa. Although he worked in a bank as a clerk, instead of using his own institution, he used one of the major money transmitters to wire transfer the funds. Because P always visited the same branch of the MTB, the employees became familiar with him. It was this familiarity that caused the employees to notice when P approached the counter with a few other men. Immediately after P transmitted his latest tranche, one of his companions also remitted monies to the same beneficiary in West Africa.

The employees found the situation odd. The next time P visited the branch, they inquired about the purpose of the transactions. He became very defensive and hostile. In addition, P's companions used their own names to transfer the money, whilst it was obvious that P was the real owner (he gave them the funds). The MTB representative decided to file a STR to the national FIU. While investigating this disclosure, the FIU could not find any incriminating evidence on P. To the contrary, he seemed to be the victim of the well-known '419 fraud'.

The investigation showed that P's companions were involved in a '419' fraud. '419' frauds involve a letter mailed or e-mailed from a foreign country. It offers the recipient the "opportunity" to share in a percentage of millions of dollars that the author is trying to illegally transfer out of the country. The recipient is encouraged to send information to the author, such as blank letterhead, bank name and account numbers, and other identifying information.

The scheme relies on convincing a willing victim to send money to the letter's author in a foreign country in several instalments of increasing amounts. The promised millions do not exist. Once the victim stops sending money, if the perpetrators have the victim's personal information, they impersonate the victim, draining his or her bank accounts and credit cards.

Warning indicators:

- Illogical activity: why would a bank clerk regularly effect wire transfers at another financial institution?
- Defensive stance in response to questioning
- Deliberate concealment of fund ownership

APPENDIX B

Streamlined Requirements for Account Opening, Provision of Financial Services and Customer Identification

The guidance in this Appendix, describes the acceptable methods of identifying individuals under the Financial Transactions Reporting Act, 2018 (FTRA) and associated Regulations.

These methods can be used to identify individuals (natural persons) who:

- seek to obtain payment services from any institution supervised by the Central Bank
- seek to open deposit facilities or obtain loan facilities on behalf of themselves;
- would like to be signatories to an account; or
- are associated with a Bahamian business or other entity.

This guidance also seeks to clarify which reliable, independent source documents, data or information can be used to verify a customer's identity per FATF Recommendation 10. It applies to business denominated in any currency, and all customers, irrespective of their residency or immigration status.

SFIs do not have to re-identify a client if they did so using the previous methods, kept the appropriate records, and have no doubts about the accuracy of information obtained. Identifying a client requires that the SFI view certain information to verify a client's identity, and ensure that the information is accurate and consistent with what is known about the client.
An account/facility will be considered "verified" if the SFI has complied with all of the applicable customer due diligence (CDD) requirements at the time of onboarding.

SFIs must now maintain at least two means of contacting the customer *(see Step 2, Points of Customer Contact for examples*). This will provide a more efficient and predictable means of managing the risk of fraud, money laundering, and other identified risks.

Is identification always required?

Payments Institutions may waive customer identification procedures when the Bahamian dollar electronic payment instrument has an initial maximum stored limit of $500, and is reloadable with up to $500 per month.[14] If at the time of issuance, an electronic payment instrument immediately (or prospectively) falls outside of these parameters, it is subject to the guidelines below.

[14] Under the Payments Instruments (Oversight) Regulations, 2017, a "Payment Institution" is defined as any Payment Service Provider other than a bank or trust company, credit union or MTB.

Process for Opening an Account or Provision of Services

Individuals can open an account as long as they meet certain conditions, and provide other critical information. This approach creates three categories of documents: A, B, and C. SFIs must complete three steps:

Step 1: Choose a combination of ID documents from a menu of options in each category
Step 2: Gather at least two means of contacting the customer
Step 3: Conduct a risk-rating of each customer (upon commencing the relationship, and on an ongoing basis using a risk-based approach).

If the person's nationality and occupation are not captured on the pieces of ID presented during Step 1, the customer may disclose that information orally or in writing. These are important risk management tools. For example, the individual may be from a jurisdiction that is high risk or subject to economic sanctions.

Step 1: The Categories Explained

- Most *Category A* documents are issued by the Government of The Bahamas, an authorized statutory body in the Bahamas, or a foreign Government. They bear some combination of a name, photograph, signature, and date of birth.

- *Category B* and *C* documents should be easily obtained by those living and working locally. They are also generally less expensive to acquire (and renew) than Category A documents. Category B includes two expired documents, namely an expired passport and driver's licence.

  Most Category B and C documents are generated, or issued, within The Bahamas. Category C documents provide a third threshold of documents to provide proof of identity.

- The Central Bank reserves the right to amend the categories as information sources evolve.

Where an identification document is listed, its electronic successor should also be acceptable. For example, a document that is paper now may subsequently become a plastic card, or part of a searchable online database.

Only originals or certified copies are acceptable. A piece of identification is considered an original if the customer received or obtained it in hand, via mail, or electronically (e.g. downloaded from a website). The document must appear valid and unmodified.

Process to Open an Account or Access Other Services—Customers with a Bahamian Connection

The commentary below applies to customers who are Bahamian, or who have a Bahamian connection, such as earning income, holding assets, or possessing residency status in The Bahamas. A later section in this document describes the requirements for international banks and trust companies wishing to open accounts for international customers with no material Bahamian connection.

The new method creates three categories of document: A, B, and C. To open a deposit account, become a signatory on a deposit account, or access a service provided by an SFI, the customer must present one of the following combinations of identification:

- 1 Valid and current Bahamian passport; or
- 1 Valid and current Bahamian driver's licence; or

- 2 items from Category A; or
- 1 item from Category A and 1 item from Category B; or
- 1 item from Category A and 1 item from Category C; or
- 1 item from Category B and 1 item from Category C.

Note: The lists below are not exhaustive. SFIs must always rely on valid and current information, or original, valid documents from independent and reliable sources.

Category A

- A certificate of Bahamian citizenship
- A certificate of naturalization
- A valid and current passport (from any jurisdiction)
- A card issued by the National Insurance Board (NIB), bearing a National Insurance Number
- A national identity card
- A permanent residence permit
- A permit to reside
- A work permit
- A resident belonger permit
- A spousal permit

Category B

- An original or official copy of a birth certificate issued by the Government of The Bahamas
- An officially (apostille) certified original or copy of a birth certificate issued by a foreign jurisdiction
- A voter's card issued by the Parliamentary Registration Department

- An expired Bahamian Passport (bearing close resemblance)
- An expired Bahamian driver's licence

Category C

- An employee identification card bearing the individual's photograph, issued by an employer with whom the SFI has a relationship.
- A mortgage or other instrument of security (original or certified copy), bearing the individual's name and residential address.
- A letter issued by The Bahamas Ministry of Education, an accredited trade school or institution of higher learning, confirming that the individual is (or was) a student.
- A Bahamas Government issued tax assessment or certificate bearing the individual's name and street address, post office box, or a description of their real property.
- A Bahamas credit reference agency search (or a copy of the results).
- A written reference from a suitable referee in the form specified by the Central Bank.

In general, there is a supervisory expectation that persons opening bank accounts in The Bahamas, or obtaining other financial services from SFIs have a material connection to the jurisdiction. This material connection is demonstrated when at least one of the items from Categories A, B, or C was issued by the Government of The Bahamas, an authorized statutory body, or generated domestically.

These requirements represent a minimum standard which SFIs must adhere to. There may be instances where additional information or documentation may be required to complete the customer profile. For example, some SFIs must determine residency for tax purposes. This can be evidenced by a utility bill, tax identification number (TIN), or its equivalent.

Where the information provided in one piece of ID does not match the information provided in another, additional information must be provided that explains the discrepancy. For example, reliable evidence of marriage, divorce, or adoption.

Who is a Suitable Referee?

A Category C "suitable referee" is a person ordinarily resident in The Bahamas who knows the customer and whom the SFI can rely on to confirm that the customer is who he or she claims to be. A suitable referee can also verify other personal details about the customer. Any of the following may be a suitable referee:

- current or former employer with whom the SFI has an existing relationship
- school principal or guidance counsellor
- licensed public accountant
- senior official at or above the rank of manager at any Central Bank SFI
- employee of the financial institution at which the service is being requested
- senior civil servant, including law enforcement officer

- doctor of medicine
- elected official
- justice of the peace or notary public
- Island Administrators or local councillor
- minister, priest, or other religious leader
- counsel and attorney-at-law
- any other individual that the Supervisory Authority (the Central Bank) may designate

Any certification or statement provided by the referee must include the following minimum details:

- customer's full name
- customer's residential address
- customer's occupation (or nature of self-employment)
- referee's name, address, occupation and contact details (such as phone number)
- how long the referee has known the customer
- a statement confirming that the referee believes the information provided about the customer to be true
- signature of the customer and referee with the date the document was signed

Step 2: Points of Customer Contact

SFIs must maintain <u>at least two</u> current means of contacting each natural person customer from the list below:

- personal email address;
- business email address (if applicable);
- mobile phone number;
- business mobile phone number (if applicable);
- personal landline number;
- business landline number (if applicable);
- personal mailing address; ▪ business mailing address;
- residential mailing address; or
- any other means of contact that the Central Bank might specify.

Any mailing address provided must include the street, post office box number (if any), city, state/province (if any), postal/zip code (if any), fixed line telephone contact (if any) and country.

For communication with minors, SFIs may also rely on direct points of contact with the individual(s) authorised to act on their behalf, such as legal parents or guardians.

There are some instances where customers may have multiple residences (e.g. one address in New Providence and another in Eleuthera, Bahamas). In these cases, it is permissible to accept more than one residential address.

SFIs must develop flexible internal procedures to verify the accuracy of the contact information provided. For example, information from a suitable referee can be used to verify the customer's

address, much like the letters from landlords and roommates. Also, items such as email addresses and mobile telephone numbers should be verified almost immediately.

Step 3: Risk Rating

All customers must be risk-rated upon commencing the relationship, and on an ongoing basis using a risk-based approach. Those customers deemed high risk will need to have their sources of funds and where appropriate, their sources of wealth, independently verified, and must produce at least one Category A document as part of their identification package. A one-size-fits-all approach to customer onboarding is inconsistent with the FATF's risk-based approach and may in effect, exacerbate the risks.

How to Identify Minors

If a child is under 18 years old, the SFI must verify the ID of the parent or guardian and record the parent's or guardian's information. The SFI can also rely on the information about the child provided by the parent or guardian. Prospective customers aged eighteen and over must be able to meet the requirements independently.

Refusal to Open Account or Provide a Service

There are several circumstances when an SFI may refuse to open an account or provide a service and still comply with this guidance:

- If the SFI has reasonable grounds to believe that the facility would be used for illegal or fraudulent purposes.
- If the SFI has reasonable grounds to believe that the individual knowingly misrepresented their personal information during the onboarding process.
- If the SFI has reasonable grounds to believe that it is necessary to refuse to open the account to protect its employees or existing customers from physical harm, harassment, or other abuse.
- If a prospective customer refuses to provide the documents or information requested.

See the full text of the AML/CFT/CPF Guidelines for related information and requirements, such as other times when a customer should be identified, and when you can rely on third parties to conduct KYC (section IV). Also, see the *Guidance Note on the Sound Management of Risks Related to Financial Crime in The Bahamas*.

International or High Net Worth Customers

The Central Bank's expectations for the identification and risk rating of international or high net worth customers are similar to the requirements for Bahamian customers. The three-step process of identifying the customer, ensuring at least two points of customer contact, and risk rating remains in place. However, this customer base typically requires a different range of products and services, some of which are higher risk for ML/TF/PF. As such:

- Every customer must present a valid passport or comparable national identification document as part of the identification process. In addition to the passport or national identification document, SFIs have, in practice, typically relied on at least one other document to identify these customers; the second document being another passport, a tax identification card/document, utility bill, etc. SFIs must be able to demonstrate there is a need to deviate from this practice as part of their risk management framework.
- SFIs must obtain independent verification of the residential address (and where relevant, the business address) of customers resident in countries where such verification is reasonably achievable. As a rule of thumb, verification is "reasonably achievable" in every country offering regular delivery of mail to individual homes and businesses.
- In limited circumstances, the equivalent of "Category C" documents may be used. These limited circumstances include customers who are minors; very young minors in particular. In such circumstances, SFIs are expected to reach a very high level of documentary confidence in the identity of their customer.

There is no expectation that any international customer possesses a Bahamian nexus.

APPENDIX C

1. DESIGNATED SANCTIONS LISTS AND SCREENING RESOURCES

Information on the status of sanctions can be obtained from websites such as European Union sanctions | EEAS

Other useful websites include:

The UK Sanctions List - GOV.UK

Sanctions List Service | Office of Foreign Assets Control

United Nations Security Council Consolidated List | Security Council

2. NON-PROFIT ASSOCIATIONS (INCLUDING CHARITIES)

For a list of all IRS recognized non-profit organizations, including charities: www.guidestar.org

For a list of registered charities: www.charity-commission.gov.uk

For various reasons, these bodies will not hold exhaustive lists.

3. POLITICALLY EXPOSED PERSONS ("PEPs")

For information on the assessment of country risks see the Transparency International Corruption Perceptions Index at www.transparency.org.

For information about recent developments in response to PEP risk, visit the Wolfsberg Group's website at www.wolfsberg-principles.com In addition, SFIs should be aware of guidance from the United States of America on enhanced scrutiny for transactions that may involve the proceeds of foreign official corruption. This is available at www.federalreserve.gov.

Additional guidance on the definitions used in Section IV C of these Guidelines can be found at: http://www.fatf-gafi.org/documents/documents/peps-r12-r22.html.

4. HIGH RISK COUNTRIES UNDER INCREASED MONITORING

A source of relevant information for SFIs is the FATF website at www.fatf- gafi.org.

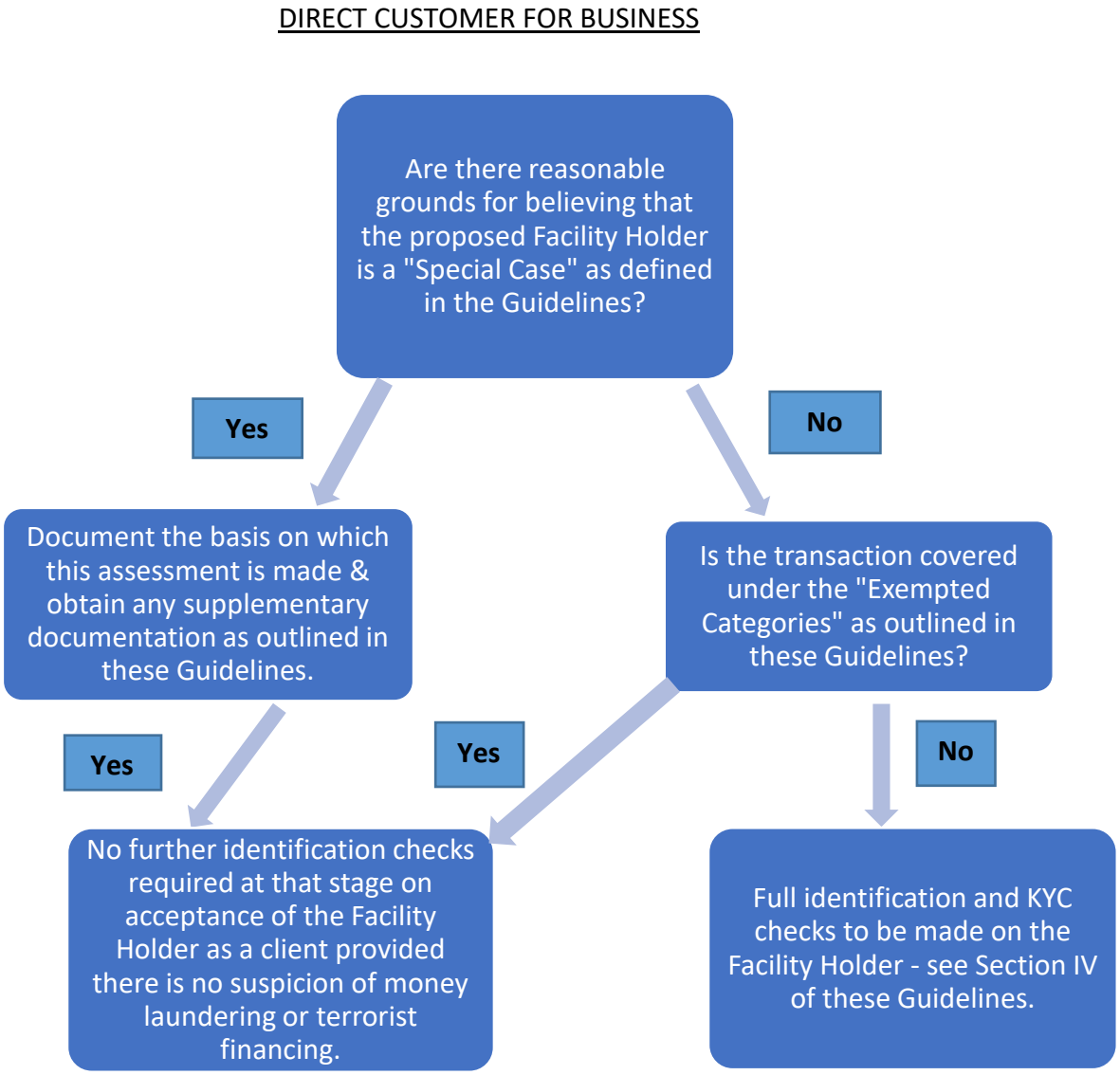
Other useful websites include:

- the Financial Crimes Enforcement Network (FinCEN) at www.ustreas.gov/fincen/ for country advisories;
- the Office of Foreign Assets Control (OFAC) at www.treas.gov/ofac for critical information pertaining to US foreign policy and national security; and
- Transparency International, www.transparency.org for information on countries vulnerable to corruption.

APPENDIX D

Anti-Money Laundering Flowchart Summary of Identification Checks

Note: This flow chart is designed as a summary document and may not be exhaustive. SFIs should refer to specific provisions within the legislation and these guidelines to ascertain the full requirements.



APPENDIX E

DEFINITION OF FINANCIAL INSTITUTION AND DESIGNATED NON-FINANCIAL BUSINESS AND PROFESSION

Section 3 of the Financial Transactions Reporting Act, 2018, defines a financial institution[15] as:

- a bank or trust company licensed under the Banks and Trust Companies Regulation Act;

- a company carrying on –

  - long term insurance business as defined in section 2 of the Insurance Act;
  - insurance business as defined in section 2 of the External Insurance Act; and
  - such other insurance business as the Minister may designate by notice in the Gazette (after consultation with the IRF Steering Committee).

- a co-operative credit union registered under The Bahamas Co-operative Credit Unions Act;

- the holder of a gaming licence, proxy gaming licence, mobile gaming licence, restricted interactive gaming licence and gaming house operator licence under the Gaming Act;

- a broker-dealer within the meaning of section 2 of the Securities Industry Act;

- a trustee, administration manager or investment manager of a superannuation scheme;

- an investment fund administrator of an investment fund within the meaning of the Investment Funds Act;

- a person whose business or a principal part of whose business consists of any of the following-

  - borrowing or lending or investing money;
  - administering or managing funds on behalf of other persons;
  - acting as trustee in respect of funds of other persons or acting in an equivalent role to a trustee in a legal arrangement similar to a trust;
  - dealing in life insurance, and insurance business, which is investment related;

[15] Individuals that carry on business as a security guard within the meaning of section 2 of the Inquiry Agents and Security Guards Act are specifically exempted from the definition of financial institution.

- providing financial services that involve the transfer or exchange of cash, including (without limitation) services relating to financial leasing, money transmissions, credit cards, debit cards, treasury certificates, bankers draft and other means of payment, financial guarantees, trading for account of others (in money market instruments, foreign exchange, interest and index instruments, transferable securities and futures), participation in securities issues, portfolio management, safekeeping of cash and liquid securities, investment related insurance and money changing; but not including the provision of financial services that consist solely of the provision of financial advice;

- a financial and corporate service provider licensed under the Financial and Corporate Service Providers Act;

- a Designated Non-Financial Business and Profession as defined in section 4 of the FTRA, 2018;

- a non-bank entity licensed and regulated by the Central Bank under the Payment Systems Act, 2012; and

- any other category of institutions that the Minister may designate by order.

Section 4 of the Financial Transactions Reporting Act, defines a designated non-financial business and profession as the business or profession of –

(a) real estate agents and brokers, when they are involved as real estate broker in financial transactions for their client concerning the buying or selling of real estate, and with respect to both the vendors and purchasers;

(b) land developer engaged in the sale or partition or condominiumizing of any part, parcel, lot or condominium unit of any larger tract or lot of land or any development of land involving the building of units sharing walls, common areas and utilities;

(c) a person whose business or any part of whose business consists of —

(i) buying for the purpose of trade, sale, exchange, or otherwise dealing in any previously owned precious metals or precious stones, whether altering the same after acquisition or not; or

(i) lending of cash on the security of previously owned precious metals or precious stones of which the person takes possession, but not ownership, in expectation of profit, gain or reward;

(d) a pay day advance provider, hire purchase lender or any lender whose loans are secured by salary deductions;

(e) a counsel and attorney or accountant when they engage in, or carry out transactions for a client concerning —

(i) the buying or selling of real estate;

(ii) a deposit or investment of cash;

(iii) the management of client funds or securities;

(iv) the management of bank, savings or securities accounts;

(v) the organisation of contributions for the creation, operation or management of a legal person;

(vi) the creation, incorporation, operation or management of a legal person or legal arrangement, and buying and selling of a business entity;

(vii) the provision of a registered office or acting as a registered agent;

(viii) the acting as or arranging for another person to act as, a nominee shareholder for another person;

(f) an accountant, but only to the extent that the accountant receives cash in the course of that person's business for the purposes of deposit or investment otherwise than as part of services rendered pursuant to a financial and corporate service provider's licence;

(g) a trust and company service providers not otherwise covered by this Act which, as a business, prepare for and carry out or otherwise provide the following services or transactions to third parties —

(i) acting as a formation, registration or management agent of legal persons;

(ii) acting as, or arranging for another person to act as, a director or secretary of a company or a partner of a partnership, or to hold a similar position in relation to other legal persons;

(iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or legal arrangement;

(iv) acting as, or arranging for another person to act as, a trustee of an express trust or performing the equivalent function for another, similar form of legal arrangement;

(v) acting as, or arranging for another person to act as, a nominee shareholder for another person;

(h) the Savings Bank as constituted under the Savings Bank Act (Ch. 315);

(i) a friendly society enrolled under the Friendly Societies Act (Ch. 313);

(j) the Bahamas Mortgage Corporation established under The Bahamas Mortgage Corporation Act (Ch. 254);

(k) the Bahamas Development Bank established under the Bahamas Development Bank Act (Ch. 357); and

(l) such other businesses and professions as the Minister may designate by Order.

(k) a counsel and attorney, but only to the extent that the counsel and attorney receives funds in the course of that person's business otherwise than as part of services rendered pursuant to a financial and corporate service provider's licence

(i) for the purposes of deposit or investment;

(ii) for the purpose of settling real estate transactions; or

(iii) to be held in a client account;

(l) an accountant, but only to the extent that the accountant receives funds in the course of that person's business for the purposes of deposit or investment otherwise than as part of services rendered pursuant to a financial and corporate service provider's licence.