AML/CFT GUIDELINES
Date Issued: May 1, 2009
Last Revised: May 31, 2017

The Central Bank of The Bahamas

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

The Central Bank of The Bahamas
The Bank Supervision Department
Frederick Street
Nassau, Bahamas

Telephone: 242-302-2615
Facsimile: 242-356-3909

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, 2000 ("BTCRA"), the Central Bank of The Bahamas Act, 2000, and The Bahamas Cooperative Credit Unions Act, 2015 ("BCCUA"). Additionally, the Central Bank has the duty, in collaboration with its SFIs, to promote and maintain high standards of conduct and management in the provision of banking and trust services.

All SFIs are expected to adhere to the Central Bank's licensing, registration and prudential requirements and ongoing supervisory programmes, including periodic onsite examinations, and required regulatory reporting. SFIs are also expected to conduct their affairs in conformity with all other Bahamian legal requirements.

The BTCRA directs the Inspector of Banks and Trust Companies ("the Inspector") to ensure that SFIs have in place strict Know-Your-Customer ("KYC") rules that promote high ethical and professional standards, and so prevent use of SFIs for criminal purposes. The Inspector is required to ensure effective offsite supervision of SFIs and is empowered to conduct onsite examinations for the purpose of satisfying himself that the provisions of, *inter alia*, the Financial Transactions Reporting Act, 2000 and the Regulations made thereunder are being complied with.

These Guidelines incorporate both the mandatory minimum requirements of the AML/CFT laws of The Bahamas and industry best practices and replace those which were initially issued by the Central Bank to SFIs in October 2005. These Guidelines also replace the Anti-Money Laundering and Anti-Terrorist Financing Handbook and Code of Practice Guidelines for Credit Unions on the Prevention of Money Laundering and Countering the Financing of Terrorism, initially issued by the Compliance Commission to credit unions in October 2013.

It is, therefore, expected that all SFIs of the Central Bank pay due regard to these Guidelines in developing responsible procedures suitable to their business to prevent money laundering and terrorist financing. If an SFI appears not to be doing so the Central Bank will seek an explanation and may conclude that the SFI is carrying on business in a manner that may give rise to sanctions under the applicable legislation.

It is important that the management of every SFI view money laundering prevention and countering the financing of terrorism as part of their risk management strategies and not simply as a stand-alone requirement that is being imposed by the legislation. Money laundering prevention and countering the financing of terrorism should not be viewed in isolation from a SFIs other business systems and needs.

These Guidelines have been prepared in consultation with those financial institutions and industry organisations that expressed an interest in being consulted in the course of the development of these Guidelines. The scope of these Guidelines covers all mainstream fiduciary, banking, lending and deposit taking activities of Central Bank Licensees.

Where a SFI is a part of an international group, it shall follow the group policy to the extent that all overseas branches, subsidiaries and associates where control can be exercised, ensure

that anti-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. Reporting procedures for suspicious transaction reports ("STR's") and the offences to which the anti-money laundering and anti-terrorism legislation in The Bahamas relates must be adhered to in accordance with Bahamian laws and practices.

The Financial Intelligence Unit ("the FIU" initially issued Guidelines in 2001 which covered anti-money laundering policies and procedures as well as requirements for suspicious transactions reporting. In 2007, the FIU updated its Guidelines to encompass matters related to the financing of terrorism, but with a narrower focus on the processes related to Suspicious Transactions Reporting (STRs). Accordingly, SFIs should continue to adhere to the FIU's Guidelines insofar as they relate to suspicious transactions reporting.

There is a risk that efforts to detect money laundering or to counter the financing of terrorism and to trace the assets will be impeded by the use of alternative undetected channels for the flow of illegal funds consequent on an automatic cessation of business (because an SFI suspected that funds stemmed from illegal activity). To avoid that risk, SFIs should report their suspicions to the FIU and obtain their own independent legal advice as to whether or not they should continue the business relationship or transaction. In carrying out transactions where a SFI is considering making a STR, the SFI should consider duties owed to third parties such as in the case of a constructive trustee. In such cases, it is recommended that independent legal advice is sought.

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 (Section IX).

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:

- the Proceeds of Crime Act, 2000 ("POCA") (as amended);
- the Anti-Terrorism Act, 2004 (as amended);
- the Financial Transactions Reporting Act, 2000 (as amended) ("FTRA");
- the Financial Transactions Reporting Regulations, 2000 (as amended) ("FTRR");
- the Financial Transactions Reporting (Wire Transfers) Regulations, 2015;
- the Financial Intelligence Unit Act, 2000 (as amended) ("FIUA"); and
- the Financial Intelligence (Transactions Reporting) Regulations, 2001 (as amended).

2 Summaries of the legislation are set out in Appendix A.

Penalties for Non-Compliance

3 SFIs should be aware that there are a number of offences which arise from failing to comply with certain obligations imposed under the Acts listed above and the Regulations made pursuant to these Acts. SFIs should also note that revisions have been effected to the laws which allow for the imposition of criminal prosecution and/or penalties. In particular, under the FIUA and The Financial Intelligence (Transactions Reporting) Regulations, where a financial institution fails to comply with the requirements of Guidelines issued by the FIU or the Central Bank, these penalties can range from a fine of $10,000 on summary conviction or $50,000 for a first offence and $100,000 for any subsequent offence on conviction in the Supreme Court. SFIs should also be aware that the Central Bank also has authority under the Financial Transactions Reporting (Wire Transfers) Regulations, to impose civil penalties of up to $2,000 for non-compliance with those laws and with these Guidelines. SFIs are, therefore, reminded to take all necessary steps to ensure full compliance with Bahamian laws.

What Is Money Laundering?

4 Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it also allows them to maintain control over those proceeds and, ultimately, to provide a legitimate cover for their source of income (see sections 40, 41 and 42 of the POCA).

The Need to Prevent Money Laundering

5 In recent years there has been a growing recognition that it is essential to the fight against crime that individuals be prevented, whenever possible, from legitimizing the proceeds of their criminal activities by converting funds from "dirty" to "clean".

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

7 Thus, The Bahamas, as a leading financial centre, has an important role to play in combating money laundering. Financial institutions that knowingly become involved in money laundering risk prosecution, the loss of their good reputation and the loss of their entitlement to operate in or from within The Bahamas.

Stages of Money Laundering

8 There is no one single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. cars or jewellery) to passing money through a complex international web of legitimate businesses and "shell" companies. Initially, however, in the case of drug trafficking and other serious crimes enforceable under the POCA, the proceeds usually take the form of cash which needs to enter the financial system by some means.

9 Despite the variety of methods employed, the laundering process is accomplished in three stages, which may comprise numerous transactions by the launderers that could alert a financial institution to criminal activity:

a) Placement - the physical disposal of cash proceeds derived from illegal activity;

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

c) Integration - the attempt 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.

10 The three basic stages may occur as separate and distinct phases. They may occur simultaneously or, more commonly, they may overlap. How the stages are used depends on the available laundering mechanisms and the requirements of the criminal organisations.

11 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; and
- transfers within and from the financial system.

Vulnerability of Financial Institutions to Money Laundering

12 Efforts to combat money laundering largely focus on those points in the process where the launderer's activities are more susceptible to recognition and have, therefore, to a large extent concentrated on the deposit taking procedures of financial institutions, i.e., the placement stage. However, it is emphasised that there are many crimes where cash is not involved. Financial institutions should consider the money laundering risks posed by the products and services they offer, particularly where there is no face-to-face contact with the customer, and devise their AML procedures with due regard to that risk.

13 The most common form of money laundering that financial institutions will encounter on a day to day basis, in respect of their mainstream banking business, takes the form of accumulated cash transactions which will be deposited in the banking system or exchanged for value. Electronic funds transfer systems increase the vulnerability by enabling the cash deposits to be switched rapidly between accounts in different names and different jurisdictions.

14 In addition, financial institutions as providers of a wide range of services are vulnerable to being used in the layering and integration stages of money laundering. Mortgage and other loan accounts may be used as part of this process to create complex layers of transactions.

14.1 Vulnerability of Credit Unions to Money Laundering and Terrorist Financing

Credit Unions, like other financial institutions that take deposits and give credit, conduct business that can be used to disguise the proceeds of crime or to finance terrorism. The money laundering or terrorist financing risk a Credit Union faces is the opportunity of a criminal to discretely place funds into that Credit Union and legitimize the funds through a series of transactions provided by the Credit Union.

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 governing 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.

The high levels of cash transactions going 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 payments are made into an account

where the amount of each deposit is unremarkable but the total credit 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.

Money launderers and terrorist financers may abuse their membership in a Credit Union to commit money laundering and/or to finance terrorism. Although Credit Unions in The Bahamas are traditionally community-based organizations, which allow the Credit Unions to be more familiar with their members and the financial services they require, the risk that members may attempt to use their membership to commit money laundering and terrorist financing still exists. Criminals may also seek to obtain membership in a Credit Union by providing a false identity or using a legitimate member to conduct risky third party transactions.

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. Therefore, they have the capacity to provide savings accounts, fixed deposits, cheque cashing, credit cards and mortgages.

Tipping Off

15 Preliminary enquiries of a customer in order to verify his identity or to ascertain the source of funds or the 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 the enquiries are likely to prejudice an investigation. Where it is known or suspected that an STR has already been filed with the FIU, the Police or other authorised agency and it becomes necessary to make further enquiries, great care should be taken to ensure that customers do not become aware that their names have been brought to the attention of the authorities.

Terrorism and Terrorist Financing

16 Terrorism is inter alia any act which is intended to intimidate the public or coerce a government or international agency to comply with the demands of terrorists and which is intended to cause death or serious bodily harm to a person, or a serious risk to public health or safety, or damage to property or interference with or disruption of essential services or systems.

17 The Anti-Terrorism Act, 2004 (as amended) defines the offence of terrorism and criminalizes the financing of terrorism. It applies to actions, persons and property both inside and outside The Bahamas. Persons who have reasonable grounds to suspect that funds or financial services are related to or are to be used to facilitate terrorism have a duty to report their suspicions to the Commissioner of Police. Failure to make a report is an offence. The Anti-Terrorism Act contains provisions empowering the Attorney General to freeze, forfeit and dispose of funds used to facilitate terrorism.

18 Terrorist financing may be derived from legitimate or illegitimate sources. It may be derived from criminal activities such as kidnapping, extortion, fraud or drug trafficking. It may also be derived from legitimate income such as membership dues, sale of publications, or income from legitimate business operations belonging to terrorist organisations.

19 Terrorist financing may involve amounts that are not always large, and the associated transactions may not necessarily be complex. However, the methods used by terrorist organisations to move, collect, hide or make available funds for their activities remain similar to those used by criminal organisations to launder their funds. This is especially so when the funds are derived from illegitimate sources, in which case, the terrorist organisation would have similar concerns to a typical criminal organisation laundering the funds. Where the funds are derived from legitimate sources, terrorist organisations would usually still need to employ the same laundering techniques to obscure or disguise the links between the organisation and the funds.

Interpretation

20 In these Guidelines, unless the context otherwise requires:

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

(b) the term "criminal conduct" includes-

(1) drug trafficking;

(2) bribery and corruption;

(3) money-laundering;

(4) any offence which may be tried in the Supreme Court of The Bahamas other than a drug trafficking offence;

(5) an offence committed anywhere that, if committed in The Bahamas, would constitute an offence in The Bahamas as set out in the Schedule to the POCA;

(6) offences under the Anti-Terrorism Act, 2004;

(7) an offence under the Gaming Act; and

(8) an offence under the Travellers Currency Declaration Act.

(c) the term "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;

(d) the term "facility holder" refers to a person in whose name the facility is established and includes any person to whom that facility is assigned or who is authorised to conduct transactions through that facility;

(e) the term "occasional transaction" refers to any one-off transaction, including but not limited to cash, that is carried out by a person otherwise than through a facility in respect of which that person is a facility holder;

(f) the term "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;

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

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

(i) the term "CDD" means customer due diligence; and

(j) 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;

(k) the term "member" means a member of a cooperative credit union; and

(l) the term "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 under the laws enforced by the Central Bank of The Bahamas.

Any other terms used throughout this document not defined herein may be found in the relevant legislation.

Responsibilities of the Central Bank

21 The fact that deposit-taking institutions are particularly vulnerable to use by money launderers and terrorists means that the Central Bank maintains a keen interest in measures aimed at countering money laundering and terrorist financing.

22 The Central Bank has informed all of its SFIs that failure to implement or maintain adequate policies and procedures relating to money laundering and terrorist financing would be taken into account in determining if the SFI continues to satisfy the criteria for licensing laid down in the BTCRA. Further, it has advised all SFIs that these Guidelines would be used as part of the criteria against which it will assess the adequacy of a SFI's systems to prevent money laundering and counter terrorist financing.

23 The POCA requires the supervisory authorities of financial institutions themselves to report any information they obtain which in their opinion indicates that any person has or may have been engaged in money laundering or terrorist financing and to disclose that information to the FIU or the law enforcement authorities.

II - INTERNAL CONTROLS, POLICIES AND PROCEDURES

24 SFIs are required to 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.

SFIs should have in place sufficient controls and monitoring systems for timely detection and reporting of suspicious activity.

24.1 An SFIs internal controls, policies and procedures shall be based on a prior risk analysis appropriate and proportionate to the nature and size of its businesses. At minimum, this analysis shall 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, products, services, and delivery channels.

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.

24.2 The risk analysis should be documented, kept up-to-date through periodic reviews and made available to the Central Bank annually.

25 All SFIs are required to establish a point of contact with the FIU in order 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 such officer is required to be registered with the FIU. SFIs are also required to appoint a Compliance Officer (CO) who shall ensure full compliance with the laws of The Bahamas (see regulation 5 of the Financial Intelligence (Transactions Reporting) Regulations, 2001).

26 All SFIs are required to:

(i) introduce procedures for the prompt investigation of suspicions and if appropriate, subsequent reporting to the FIU;

(ii) ensure that the MLRO, the CO, and any other persons appointed to assist them, have timely access to systems, customer records and all other relevant information which they require 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 Officer;

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

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

CO.

27 A SFI may choose to combine the functions of the CO and the MLRO depending upon the scale and nature of its business. The roles might be assigned to its inspection, fraud or compliance functions.

28 SFIs are required to:

(a) have AML/CFT policies, controls and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that they have identified or which have been identified by the Central Bank or other relevant authorities in The Bahamas;

(b) monitor, compliance with internal AML/CFT policies, procedures, and controls, and enhance them, if necessary;

(c) take enhanced measures to manage and mitigate the risks where higher risks are identified; and

(d) where appropriate, having regard to the size and nature of their business, engage an independent audit function to test the internal policies, controls and procedures referred to in paragraph (a).

29 SFIs should also establish and implement appropriate policies and procedures to ensure high standards are being followed when hiring employees. To this end, SFIs should have in place screening procedures, which should involve making diligent and appropriate enquiries about the personal history of the potential employee and taking up appropriate references on the individual.

29.1 For the purposes of paragraphs 29.2 to 29.5, a reference to SFI means a SFI incorporated in The Bahamas.

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

29.3 Subject to the SFI putting in place adequate safeguards to protect the confidentiality and use of any information that is shared, and to the extent permitted by the laws of the countries or jurisdictions that its branches and subsidiaries are in, a SFI shall 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 money laundering and terrorism financing risk management.

29.4 Where the AML/CFT requirements in the host country or jurisdiction differ from those in The Bahamas, SFIs shall 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.

29.5 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 shall apply appropriate additional measures to manage the money laundering and terrorism financing 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

30 In its paper issued in October 2001 on Customer Due Diligence for Banks, the Basel Committee on Banking Supervision recognised that adequate KYC policies and procedures have particular relevance to the safety and soundness of banks, in that such policies:

(i) prevent reputation risk and preserve the integrity of the banking system by preventing the use of the bank for criminal purposes; and

(ii) complement the risk management strategy of banks (by enabling them to identify, limit and control risk exposure in assets and liabilities).

31 Similarly, the Financial Action Task Force ("FATF"), in its revised 40 Recommendations on Anti-Money Laundering and Combating the Financing of Terrorism, issued in February 2012, also recommends that financial institutions adopt a risk based approach to customer due diligence.

32 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. This approach is in keeping with international best practices.

Developing a Risk Rating Framework

33 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.

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

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

(ii) 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);

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

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

35 The risk rating framework should provide for the periodic review of the customer relationship to allow the SFI to determine whether any adjustment should be made to the risk rating. The review of the risk rating for high risk customers may be undertaken more frequently than for other customers and a determination made by senior management as to how the heightened risks are to be managed and mitigated; and failing same whether the relationship should be continued. All decisions regarding high risk relationships and the basis for these decisions should be documented.

36 The risk rating framework should take into account customer acceptance and on-going monitoring policies and procedures that assist the SFI in identifying the types of customer that are likely to pose a higher than average risk of money laundering or funding of terrorist activities. A more extensive customer due diligence process should be adopted for higher risk customers. There should also be clear internal guidelines on which level of management is able to approve a business relationship with such customers. The risk rating framework should provide for documentation of any changes in a customer's risk rating and the reason(s) for such change. In determining the risk profile of any customer, SFIs should take into account factors such as the following risk criteria (which are not set out in any particular order of importance 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.

37 **Prospective Customers**

SFIs should assess the potential risk inherent in each new client relationship prior to establishing a business relationship. This assessment should take account of whether and to what extent a customer may expose the SFI to risk, and of the product or facility to be used by the customer. Based on this assessment, the SFI should decide whether or not to establish a facility for the customer concerned, or to continue with it.

38 **Existing Customers**

SFIs are required to risk rate all client relationships; including those in existence prior to 29th December, 2000 ("existing customers"). SFIs should review the KYC documentation in relation to their existing customers to ensure compliance with the FTRA, the FTRR, any other applicable laws of The Bahamas, and the SFI's internal KYC requirements. All risk ratings should be documented.

IV - VERIFICATION OF CUSTOMER IDENTITY

39 Identity generally means a set of attributes which uniquely define a natural or legal person. There are two main constituents of a person's identity and for the purposes of these Guidelines the two elements are:

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

(b) the activity undertaken**.**

What is required

40 SFIs are required to:

(a) identify the customer and verify that customer's identity using reliable, independent source documents, data or information; and
(b) verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person.

Nature and Scope of Activity

41 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.

42 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 C for a flow chart summary of the different steps involved.

43 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.

44 Normally the prospective customer should be interviewed personally. 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, an explanation should be sought and the SFI:

(i) must not commence or continue the business relationship as the case may be,

(ii) must not undertake any transaction for the customer, issue documents of title or remit income (though it may be re-invested), and

(iii) must consider whether a report to the FIU ought to be made.

45 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 as opportunities arise. SFIs should refer to paragraphs 60 - 63 of these

guidelines for guidance on when further verification of a customer's identity may be necessary.

46 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.

WHO SHOULD SFIs VERIFY & WHEN SHOULD IDENTITY BE VERIFIED?

Facility Holder

47 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 are used interchangeably and who this is will vary. SFIs should 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 such customers to become facility holders;

(b) whenever the amount of cash involved in an occasional transaction exceeds $15,000, the identity of the person who conducts the transaction should be verified before the transaction is conducted;

(c) whenever the amount of cash involved in an occasional transaction exceeds $15,000 and it appears to a SFI that the person conducting the transaction is doing so on behalf of any other person or persons. In these circumstances the identities of the third parties must be verified before the transaction is conducted;

(d) whenever it appears that two or more (occasional) transactions are or have been deliberately structured to avoid lawful verification procedures in respect of the person(s) conducting the transaction(s) and the aggregate amount of cash involved in the transaction(s) exceeds $15,000. Verification should be conducted as soon as practicable after the SFI becomes aware of the foregoing circumstances;

(e) whenever a SFI knows, suspects or has reasonable grounds to suspect that a customer is conducting or proposes to conduct a transaction which:

- involves the proceeds of criminal conduct as defined in the POCA; or
- is an attempt to avoid the enforcement of the POCA

verification should take place as soon as practicable after the SFI has knowledge or suspicion in respect of the relevant transaction; and

(f) whenever a SFI has reasonable grounds to suspect that funds as defined in the Anti-Terrorism Act, 2004 or financial services are related to, or are to be used to facilitate an offence under the Anti-Terrorism Act, verification should take place as soon as practicable after such suspicions arise.

48 Where satisfactory evidence of identity is required, no transaction should be conducted over the facility pending receipt of identification evidence and information. Documents of title should not be issued, nor income remitted (though it may be re-invested) in the absence of evidence of identity.

IDENTIFICATION PROCEDURES

A. Natural Persons

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

(i) full and correct name/names used;

(ii) correct permanent address including postcode (if appropriate);

(iii) date and place of birth; and

(iv) purpose of the account and the nature of the business relationship.

50 The following information may also be required when SFIs seek to verify identity:

(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; and

(iv) source of funds.

51 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 Name and Address

52 One or more of the following steps is recommended to confirm addresses:

- checking the Register of Electors;
- provision of a recent utility bill, tax assessment or bank or credit union statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined);

- checking the telephone directory; and
- record of home visit.

53 The information obtained should demonstrate that a person of that name exists at the address given, and that the facility holder is that person.

54 Both residence and 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 any other official body or government that would prohibit such business being transacted. (SFIs should refer to Appendix B for a list of websites which contain information on the status of sanctions.)

55 Obtaining a customer's date of birth provides an extra safeguard if, for example, a forged or stolen passport or driver's licence is used to confirm the identity which bears a date of birth that is clearly inconsistent with the age of the person presenting the document.

56 Confirmation of a person's address and/or nationality is also useful in determining whether a customer is resident in a high-risk country.

57 Information and documentation should be obtained and retained to support, or give evidence of the details provided by the facility holder.

58 Identification documents, either originals or certified copies, should be pre-signed and bear a discernable photograph of the applicant. For example:

(a) current valid passport;

(b) armed forces ID card;

(c) drivers licence bearing the photograph and signature of the applicant;

(d) voter's card;

(e) national identity card; or

(f) such other documentary evidence as is reasonably capable of establishing the identity of the individual customer.

59 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?

60 Where a customer's identity has been verified, further verification is mandatory if:

(a) during the course of the business relationship the SFI has reason to doubt the identity of the customer;

(b) a SFI knows, suspects or has reasonable grounds to suspect that a customer is conducting or proposes to conduct a transaction which:

- involves the proceeds of criminal conduct as defined in the POCA; or

- is an attempt to avoid the enforcement of the POCA; (in such cases, verification should take place as soon as practicable after the SFI has knowledge or suspicion in respect of the relevant transaction);

(c) there is a material change in the way a facility is operated.

61 It is also recommended that where the circumstances of paragraph 47(f) arise, re-verification should be carried out in respect of those customers. 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.

62 SFIs may also as part of their own internal AML/CFT 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.

63 The need to confirm and update information about identity, such as changes of address, and the extent of additional KYC information to be collected over time will differ between SFIs. It will also depend on the nature of the product or service 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

64 Most people need to make use of the financial system at some point in their lives. It is important, therefore, that the elderly, the disabled, students and minors, or the socially or financially disadvantaged should not be precluded from obtaining

financial services just because they do not possess the usual types of evidence of identity or address, such as a driver's licence or passport where they cannot reasonably be expected to do so. Internal procedures must allow for this, and must provide appropriate advice to staff on how identity can be confirmed in these exceptional circumstances manager may authorise the opening of a business relationship if the manager is satisfied with confirmation of identity in these limited circumstances but 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.

65 In particular, domestic SFIs, may exercise discretion and flexibility without compromising sufficiently rigorous AML/CFT procedures, in instances where a government-issued identification document is unavailable. 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). The important point is that a person's identity can be verified from an original or certified copy of another document, preferably one with a photograph.

66 In these cases it may be possible for the SFI to accept confirmation from a professional (e.g. doctor, lawyer, etc.) who knows the person. Where the individual lives in accommodation for which the person is not financially responsible, or for which there would not be documentary evidence of the person's address, it may be acceptable to obtain a letter from the Department of Social Services or a similar organisation as confirmation of such person's address.

67 For students or other young people, the normal identification procedures set out above should be followed as far as possible. Where such procedures would not be relevant, or do not provide satisfactory evidence of identity, verification might be obtained in the form of the home address of parent(s), by making enquiries of the Applicant's college or university or in the absence of a passport, a birth certificate will suffice. However, care should be taken around the beginning of the academic year before a student has taken up residence at the place of education as registration frauds are known to occur.

68 Under normal circumstances, a family member or guardian who has an existing relationship with the SFI concerned would introduce a minor. 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.

69 SFIs should also take appropriate steps to verify the name and address of applicants by one or more methods, e.g.:

(i) obtaining a reference from a "respected professional" who knows the applicant;

(ii) checking the voter's card;

(iii) making a credit reference agency search;

(iv) checking a local telephone directory;

(v) requesting sight of a recent real property tax bill, local authority tax bill, utility bill, bank, credit union or trust company statement. (To guard against forged or counterfeit documents, care must be taken that the document is an original and not a copy); or

(vi) a personal visit to the home of the applicant where possible.

70 The term "respected professional" could refer to, for instance, lawyers, accountants, directors or managers of a regulated SFI, priests, ministers of religion, doctors or teachers.

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

A4. Certification of Identification Documents

72 SFIs should exercise due 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.

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

74 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.

75 A certifier must be a suitable person; such as those below. The following list of suitable certifiers is not intended to be exhaustive, and a SFI is not 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.

76 The certifier should sign the copy document (printing 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

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

(iii) 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 paragraphs 49(i) – (iii) and 50(i) and (ii) of these Guidelines;

(iv) 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 paragraphs 49(i) – (iii) and 50(i) and (ii) of these Guidelines; and

(v) 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;

78 In addition, it is strongly recommended that SFIs obtain the following information and documents when seeking to verify the identity of corporate clients:

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

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

(a) date of commencement of business;

(b) products or services provided;

(c) location of principal business; and

(d) name and location of the registered office and registered agent of the corporate entity, where appropriate;

(iii) the reason for establishing the business relationship;

(iv) 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;

(v) 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;

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

(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;

(viii) 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

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

79 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 paragraphs 49 (i)-(iii), 50, (i) and (ii) and where appropriate, monitor the ongoing business relationship more closely.

80 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 72 to 75 of these Guidelines.

81 Trading companies may sometimes form part of complex organisational structures which also involve trusts and foundations. Particular care should be taken to verify the legal existence of the corporate entity and to ensure that any person purporting to act on behalf of the corporate entity is authorised to do so. The principal requirement is to look behind a corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the company. Enquiries should be made to confirm that the company 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.

82 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.

83 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.

84 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.

85 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

86 Where the corporate client is a segregated accounts company, SFIs should have regard to the guidance for corporate clients (paragraphs 77 to 85). In addition to the documents and information set out in paragraphs 77 and 78, 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

87 The authority to deal with assets under a power of attorney constitutes a business relationship and 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 49 and 50. 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

88 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 of a firm or business, in line with the requirements in these Guidelines for individual customers (see paragraphs 49 to 51).

(ii) identification evidence for all authorised signatories, in line with the requirements in these Guidelines for individual customers (see paragraphs 49 to 51). 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 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.

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

90 The following information may also be required when SFIs seek to verify the identity of partnerships and unincorporated businesses:

(i) description and nature of the business including:

(a) date of commencement of business;

(b) products or services provided; and

(c) location of principal place of business;

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

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

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

(c) an indication of 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;

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

(g) 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

(h) 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

91 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.

92 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 paragraphs 49 to 59;

(ii) where a FCSP or their underlying clients are companies, SFIs should follow the guidance set out in paragraphs 77 to 85, and

(iii) where a FCSP is or their underlying clients are partnerships or unincorporated associations, SFIs should follow the guidance set out in paragraphs 88 to 90.

93 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

94 Legal structures such as trusts and foundations, and nominee and fiduciary accounts can be used by criminals who wish to mask the origin of funds derived from crime if the trustee or fiduciary does not carry out adequate procedures. Particular care is needed on the part of the SFI when the facility holder is a trustee or fiduciary who is not an Exempted Client (see paragraph 137) or an Eligible Introducer (see paragraphs

128 and 129). The principal means of preventing money laundering and terrorist financing through the use of legal structures, nominee companies, and fiduciaries is to verify the identity of the provider of funds, such as the settlor and also those who have control over the funds, that is to say, the trustees, advisors, and any controllers who have the power to remove the trustees/advisors etc. It should be borne in mind that the settlor may also be a sole trustee or a co-trustee of the trust, in which case, identification documentation should be obtained in relation to him.

95 The SFI should normally, in addition to obtaining identification evidence for the trustee(s) and any other person who has signatory powers on the account:

(i) make appropriate enquiry as to the general nature and the purpose of the legal structure and the source of funds;

(ii) obtain identification evidence for the settlor(s) and for 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).

(iii) in the case of a nominee relationship, obtain identification evidence for the beneficial owner(s).

96 Where the settlor is deceased, written confirmation should be obtained for the source of funds in the form, for example, of Grant of Probate, and/or copy of the will creating the trust.

97 Where a corporate trustee acts jointly with a 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. Corporate trustees should also hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors and ensure that such information is kept as up to date as possible.

98 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 authorised signatories to the bank account should also be verified.

99 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 cause the need of further enquiries.

100 SFIs are also required by the FTRA to verify the identity of any underlying beneficiary of a legal structure. It is recognized that it may not be possible to identify the beneficiaries of trusts precisely at the outset. 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, verification must be carried out by the SFI providing the facility unless the transaction is or has been introduced by another financial institution (see the section *"Reliance on Third Parties to Conduct KYC on Customers"* for further guidance) on behalf of the settlor and beneficiary and such financial institution is itself required to verify the identity of the settlor and beneficiary. Verification must be conducted prior to making a distribution to the beneficiary or when the beneficiary intends to exercise vested rights.

101 SFIs should be particularly vigilant where there is no readily apparent connection or relationship of the settlor to the beneficiaries of a trust. Since the economic nature of a trust is a mechanism for the settlor to benefit a beneficiary, typically, not in return for any consideration (payment, transfer of assets or provision of services), SFIs should endeavour so far as possible to ascertain the settlor's reasons for wanting to benefit a beneficiary with whom he seemingly has no connection. This can be a matter of great sensitivity (for example where the beneficiary turns out to be a child of the settlor born out of wedlock) and SFIs are encouraged to take this into account while pursuing necessary or appropriate inquiries.

There are a number of commercial structures in which a trust may feature as the legal owner, such as in debt repackaging arrangements or aircraft leasing structures. In such cases where the traditional relationship between the settlor and beneficiary is absent, SFIs should demonstrate that they understand the commercial rationale for the arrangement and have verified the identity of the various counterparties.

H. Identification of New Trustees

102 Where a trustee whose identity has been verified is replaced, the identity of the new trustee should be verified before the new trustee is allowed to exercise control over funds.

I. Foundations

103 It will normally be necessary to obtain the following documented 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 should be obtained in order to confirm the existence and legal standing of the foundation;

(iii) the source of funds SFIs should obtain and 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 providing the funds for the foundation and/or for whom a founder may be acting in accordance with paragraphs 49 to 59; and

(iv) SFIs should obtain 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 paragraph 49 (i) – (iii), 50 (i) and (ii) 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 77 to 85; where the founder is an individual, SFIs should follow the guidance provided in paragraphs 49 to 59.

104 Identification evidence should also be obtained for all vested beneficiaries of the foundation.

J. Executorship Accounts

105 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.

106 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.

K. Non-Profit Associations (Including Charities)

107 Non-profit associations may pose specific 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 not known and as a result neither is the source of the funds.

108 Where the entity is a corporate entity the account opening procedures should be in accordance with the procedures for corporate clients set out in paragraphs 77 to 85 in the case of Trusts the procedures in paragraphs 94 to 102; and in the case of Foundations the procedures in paragraphs 103 and 104 should be followed.

109 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.

110 Where a non-profit association is registered as such in an overseas jurisdiction, it may be useful for the SFI to contact the appropriate 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.

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

112 Whilst it is not practical 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 166 and 167 below).

L. Products and Services Requiring Special Consideration

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

(a) Provision of Safe Custody and Safety Deposit Boxes

114 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) New Products, Practices and Technological Developments

115 SFIs should have policies in place and take such measures as may be needed to identify and assess the money laundering and terrorist financing 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.

115.1 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 money laundering or terrorism financing risks, to manage and mitigate those risks.

115.2 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.

(c) Intermediaries

116 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 128 and 129 of these Guidelines and/or is from a country that is not listed in the First Schedule of the FTRA (see Appendix D for a list of First Schedule countries). 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 127 and 128, such verification is not required.

(d) Occasional Transactions

117 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.

118 The FTRA defines an "occasional transaction" as any one-off transaction including but not limited to cash, that is carried out by a person otherwise than through a facility in respect of which that person is a facility holder.

119 Customers who conduct occasional transactions (whether a single transaction or a series of linked transactions) where the amount of the transaction or the aggregate of a series of linked transactions is less than $15,000 or the equivalent in any other currency, are exempt from the full verification requirements of the FTRA.

120 SFIs need to be aware at all times of any cases where the total of a series of linked transactions exceeds the prescribed limit of $15,000 and they should verify the identity of the customer in such cases. These are cases where in respect of two or more occasional transactions it appears at the outset, or at a later stage, to a person handling any of the transactions that the transactions are linked and that the aggregate amounts of these transactions exceed or are likely to exceed $15,000.

121 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.

122 Verification of identity will not normally be needed in the case of an exempted occasional transaction referred to above. If, however, the circumstances surrounding the occasional transaction appear to the SFI to be unusual or questionable, further enquiries should be made. If as a result of enquiries, the SFI becomes aware of or suspects money laundering or the financing of terrorism the SFI must, in accordance with section 10(A)(1) of the FTRA, take steps to verify the proposed client's identity. Where money laundering is known or suspected, the SFI should make a suspicious transaction report in line with Section 14(1) of the FTRA regardless of the size of the transaction. Where terrorist financing is known or suspected, the SFI should make a report to the Commissioner of Police.

RELIANCE ON THIRD PARTIES TO CONDUCT KYC ON CUSTOMERS

123 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 itself.

124 There are, however, certain circumstances in which 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 (See section 8(6) and 9(6) FTRA).

125 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 (see section 11(3) and 11(4) FTRA).

126 This exemption applies only to occasional transactions and transactions conducted by financial institutions that are facility holders of SFIs (see sections 7, 8 and 9 of the FTRA). 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

127 Where a business relationship is being instituted the SFI is obliged to carry out KYC procedures on any client introduced to it by another financial institution unless the financial institution is an eligible introducer able to provide the SFI with copies of all documentation required by the SFI's KYC procedures.

128 Recent amendments to the FTRA extends the categories of financial institutions that may act as eligible introducers subject to the directions and guidance issued by the Central Bank as the relevant Supervisory Authority. In accordance with these amendments, the Central Bank requires that to be an eligible introducer for a SFI, 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 2011; or

(iv) an investment fund administrator licensed under the Investment Funds Act, 2003).

129 A foreign financial institution may also 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 128 (i) to (iv) above and be based in a country listed in the First Schedule of the FTRA

(ii) it must be subject to equivalent or higher AML/CFT 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.

130 Where a third party satisfies the definition of eligible introducer, a SFI may place reliance upon the KYC procedures of the eligible introducer but remains ultimately responsible for ensuring that adequate due diligence procedures are followed and that the documentary evidence of the eligible introducer that is being relied upon, is satisfactory for these purposes. Satisfactory evidence is evidence that the eligible introducer is subject to AML/CFT standards of regulation that are equivalent to or higher than such standards provided under Bahamian law. Only senior management should take the decision that reliance may be placed on the eligible introducer and the basis for deciding that normal due diligence procedures need not be followed should be part of the SFI's risk-based assessment.

131 Notwithstanding any reliance on an eligible introducer's KYC procedures, 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

132 The obligation to maintain procedures for obtaining evidence of identity is general, but paragraphs 133 to 137 set out a number of exemptions and concessions.

A. Bahamian or Foreign Financial Institutions

133 Verification of identity is not normally required when the facility holder is one of the financial institutions referred to in paragraphs 128 or 129. 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 standards of regulation as provided for in Bahamian law.

134 In all cases, the SFI must be satisfied that it can rely upon the eligible introducer. The SFI may 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.

135 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. Occasional Transactions: Single or Linked

136 Verification of identity is not normally needed in the case of a single occasional transaction when payment by, or to, the customer is less than $15,000. Irrespective of the size of a transaction however, any suspicions of money laundering must be reported in accordance with the FIU's Suspicious Transactions Reporting Guidelines. Suspicions of terrorist financing must be reported to the Commissioner of Police. SFIs should also have regard to paragraphs 117 to 122 of these guidelines when dealing with occasional transactions.

C. Exempted Clients

137 Documentary evidence of identity will not normally be required in the case of:

(i) superannuation schemes;

(ii) occupational retirement/pension plans which do not allow non-employee participation;

(iii) financial institutions regulated by the Central Bank, the Securities Commission, the Office of the Registrar of Insurance Companies ("the Registrar of Insurance"), or the Gaming Board;

(iv) foreign financial institutions located in a jurisdiction specified in the First Schedule of the FTRA, which is regulated by a body having equivalent regulatory and supervisory responsibilities as the Central Bank the Securities Commission, the Registrar of Insurance, or the Gaming Board; any central or local government agency or statutory body;

(v) 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;

(vi) a regulated Investment Fund as defined in section 2 of the Investment Funds Act, 2003 or regulated Investment Fund located in a country specified in the First Schedule of the FTRA and regulated by a body having equivalent regulatory and supervisory responsibilities as the Securities Commission;

(vii) an applicant for insurance consisting of a policy of insurance in connection with a pension scheme taken out by virtue of a person's contract of employment or occupation;

(viii) an applicant for insurance in respect of which a premium is payable in one instalment of an amount not exceeding $2,500;

(ix) an applicant for insurance in respect of which a periodic premium is payable and where the total payable in respect of any calendar year does not exceed $2,500; and

(x) any Bahamian dollar facility of or below $15,000.

138 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 money laundering or terrorist financing is known or suspected. If money laundering is known or suspected then a report must be made to the FIU. Knowledge or suspicion of terrorist financing should be reported to the Commissioner of Police. In both cases verification procedures must be undertaken if this has not already been done.

Where a SFI has taken a decision to apply simplified CDD measures, the SFI must retain documentation that supports the basis for arriving at this decision.

ENHANCED DUE DILIGENCE

139 SFIs should apply enhanced CDD measures on a risk sensitive basis for such categories of customer, business relations or transactions as the SFI may assess to present a higher risk for money laundering or terrorist financing. As a part of this, a SFI may conclude, under its 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.

140 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 hold 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.

141 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 persons (natural or legal persons) from or in countries and jurisdictions known to have inadequate AML/CFT

measures including, in all cases, those countries in relation to which the Financial Action Task Force (FATF) requires the application of enhanced due diligence measures. (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

142 SFIs should consider the money laundering and terrorist financing risks posed if there is no face-to-face contact with prospective customers when establishing customer relationships and when conducting ongoing due diligence on existing customers. This would include assessing the possibility that a customer is deliberately avoiding face-to-face contact.

143 Non face-to-face transactions carry an inherent risk of forgery and fraud, which SFIs should take care in their internal systems, policies and procedures to mitigate. The extent of verification in respect of non-face-to-face customers will depend on the nature and characteristics of the product or service provided and the assessed money laundering and terrorist financing risk presented by the customer.

144 Where a customer approaches a SFI by post, telephone, transmission of instructions or applications via facsimile or similar means, or over the internet, and it will not be practical to seek sight of a passport or other photographic identification document, verification of identity should be sought from a financial institution in a country listed in the First Schedule of the FTRA (see Appendix D) and that is subject to equivalent or higher AML/CFT standards of regulation as provided for by Bahamian law.

145 Where the customer has not been physically present for identification purposes, a SFI should take specific and adequate measures to compensate for the higher risk most notably for forgery and fraud, for example, by applying 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 listed in the First Schedule to the FTRA;

(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.

146 Any subsequent change to the customer's name, address, or employment details of which the SFI becomes aware should be recorded and also be regarded as a "trigger" event. Generally a KYC review would be undertaken as part of good business practice and due diligence process but it would also serve for money laundering or terrorist financing prevention.

147 File copies of supporting evidence should 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.

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

B. Correspondent Relationships

149 For the purposes of this section B –

"correspondent relationships" means the provision of correspondent banking services by a bank in The Bahamas as the correspondent to a respondent financial institution, including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services;

"respondent financial institution" means a bank or financial institution, outside The Bahamas to which correspondent banking or other similar services are provided; and

"other similar relationships" include relationships established for securities transactions or funds transfers.

150 SFIs should obtain senior management approval before establishing new correspondent and other similar relationships and a review of these relationships should be conducted at least annually.

151 Transactions conducted through correspondent and other similar relationships need to be monitored according to perceived risk. SFIs should assess AML/CFT controls to ascertain that they are adequate and effective, having regard to the AML/CFT measures of the country in which the respondent operates.

152 Additionally, SFIs must gather sufficient information about the respondent's business to understand fully the nature of the respondent's business 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.

153 SFIs should document the respective AML/CFT responsibilities of each institution in.

154 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.

155 The volume and nature of transactions from high risk jurisdictions flowing through respondent accounts provided by SFIs, or those with material deficiencies should be monitored against expected levels and destinations, and any material variances should be explored.

156 Staff dealing with correspondent banking accounts should be trained to recognise high risk circumstances, and be prepared to challenge respondents over irregular activity, whether isolated transactions or trends, submitting an STR where appropriate.

157 Where the correspondent or other similar relationship involves a payable-through-account, SFIs should take reasonable steps to satisfy themselves that sufficient due diligence has been undertaken by the remitting bank on the underlying client and the origin of funds. In these circumstances, the Licensee must be satisfied that the respondent financial institution is able to provide KYC documentation on the underlying customer, upon request.

158 SFIs should consider terminating 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

159 For the purposes of this section C -

"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;

"domestic politically exposed person" means a natural person who is or has been entrusted domestically with prominent public functions;

"foreign politically exposed person" means a natural person who is or has been entrusted with prominent public functions in a foreign country;

"immediate 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;

"international organisation politically exposed person" means a natural person who is or has been entrusted with prominent public functions in an international organisation;

"politically exposed person or PEP" means a domestic politically exposed person, foreign politically exposed person or international organisation politically exposed person who hold or have held, in the preceding year, prominent public positions; 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 immediate family members and close associates of all types of PEPs. The definitions in this paragraph are drawn from the FATF Recommendations. For further guidance SFIs should refer to Appendix B for a list of websites relevant to PEPs.

Provision of financial services to corrupt PEPs exposes SFIs to reputational risk and costly law enforcement measures.

160 SFIs are encouraged to be vigilant in relation to PEPs from all jurisdictions, in particular High Risk Countries (see paragraphs 166 and 167), who are seeking to establish business relationships. In relation to foreign PEPs, in addition to performing normal due diligence measures, SFIs should, using a risk sensitive approach:

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

(ii) have developed 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;

(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.

In the context of this risk analysis, it would be appropriate if SFIs focused their resources on products and transactions that are characterised by a high risk of money laundering.

161 SFIs may adopt a risk-based approach in determining whether to perform the enhanced CDD measures as set out in paragraphs 160 (ii) through (iv) and 164, 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 Licensee present a higher risk for money laundering or terrorism financing.

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

163 SFIs should develop and maintain " enhanced scrutiny" practices which may include the following measures, to address PEPs risk:

(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 information set out in Appendix B). SFIs which are part of an international group might also use the group network as another source of information;

(ii) where SFIs entertain 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, such as, but not limited to trading or dealing in precious stones or precious metals.

164 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 and multiple jurisdictions);

(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 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.

165 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 B for a list of websites relevant to the risks associated with PEPs.

D. High-Risk Countries

166 Certain countries are associated with predicate crimes such as drug trafficking, fraud and corruption and with terrorist financing and consequently pose a higher potential risk to SFIs. Conducting business relationships with customers who are either citizens of or domiciled in such countries exposes the SFI to reputational risk and legal risk. SFIs are encouraged to consult publicly available information to ensure that they are aware of countries/territories identified as having weaknesses in their AML/CFT systems and which may pose a higher risk. SFIs should refer to Appendix B for a list of relevant websites.

167 Caution should also be exercised in respect of the acceptance of certified documentation from individuals and entities located in high-risk countries and territories and appropriate verification checks undertaken on such individuals/entities to ensure their legitimacy and reliability.

E. Bearer Shares

168 When assessing the risk of a particular relationship, SFIs should consider whether any legal person who is the customer, beneficial owner or underlying principal has issued or has the potential to issue bearer shares. Bearer shares can provide a significant level of anonymity which can be abused by those seeking to use companies for a criminal purpose.

In circumstances where such a relationship has been identified, and in order to address the specific risks of such a relationship, SFIs should undertake the following enhanced CDD measures to ensure that the standard evidence of identity is obtained and that customers who have issued or have the potential to issue bearer shares, are not misused for money laundering and/or terrorist financing:

1. Only open accounts for companies capable of issuing bearer shares where the holders and beneficial owners of those shares are verified in accordance with the guidance under the section "IDENTIFICATION PROCEDURES".

2. Establish procedures to ensure that they are notified whenever there is a change of holder and/or beneficial owner. As a minimum, these procedures should require SFIs to take the following measures:

   (a) obtain an undertaking in writing from the beneficial owner which states that immediate notification will be given to the SFI if the shares are transferred to another party;
   (b) ensure that where bearer shares are not held by the SFI, that they are held in secure custody by a named custodian which has undertaken to inform the SFI of any proposed change in ownership of the company or of any changes to records relating to these shares and the custodian, and
   (c) depending on its risk assessment of the customer, having the undertaking certified by an accountant, lawyer or equivalent professional.

TREATMENT OF BUSINESS RELATIONSHIPS EXISTING PRIOR TO 29th DECEMBER, 2000

169 Section 6(6) of the FTRA, provides that financial institutions are required to verify the identity of customers who have facilities which were established prior to 29th December, 2000 ("existing facilities"). Where an SFI had not verified the identity of any such customer ("existing customers") by 1st April 2004, the SFI was required to notify the Central Bank not later than 30th April, 2004. SFIs should have regard to the paragraphs which follow when dealing with existing customers.

170 It is clear that certain business relationships established prior to the enactment of the FTRA (29th December, 2000) can still present a major threat of money laundering or terrorist financing, and indeed, it is a widely recognised tactic for money launderers to establish seemingly legitimate and normally-run accounts which are then used for laundering money or financing terrorism at a later date.

171 In accordance with section 6(6) of the FTRA, 2000, the Central Bank directed SFIs to complete the verification of existing client identity, in the case of domestic retail business, by 30th June, 2006 and in the case of all other business by 31st December, 2005. SFIs which did not implement appropriate measures to satisfy the verification requirements of section 6(6) of the FTRA by these dates, were required to take steps to suspend or terminate the business relationship.

172 SFIs are reminded of the reporting duties imposed by the FTRA with respect to suspicious transactions. Where a customer refuses to provide information for his

identity to be verified in accordance with the verification requirements of Section IV, this may be a circumstance that should put the SFI on enquiry as to whether the reason for non-cooperation may be that the business relationship is being used for money laundering purposes or to finance terrorism.

173 In those cases where persons do not have 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 give comfort provided that the conditions of paragraph 64 are satisfied and that the introduction can never replace the address verification procedures described in these Guidelines. Details of who initiated the account and authorized the introduction must be kept. Directors/Senior Managers should take a common sense approach in determining whether certain documents should be waived in any particular situation. Where specific documentation of a customer is waived, management must document why the waiver was granted.

174 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 or address. However, the opportunity should be taken to confirm the relevant customer information. This is particularly important if there has been no recent contact or correspondence with the customer e.g. within the last twelve months or when a previously dormant account has been reactivated.

ON-GOING MONITORING OF BUSINESS RELATIONSHIPS

175 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

176 SFIs are expected to have systems and controls in place to monitor on an ongoing basis relevant account activities in the course of the business relationship. 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. The purpose of this monitoring is for SFIs to be vigilant to note any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts. Possible areas to monitor could be:

(a) transaction type;

(b) frequency;

(c) amount;

(d) geographical origin/destination; and

(e) account signatories.

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

Depending on the type of business each Licensee conducts and the nature of its client portfolio, each 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 sound practices, such as periodic on-site visits, interviews with the business's management, or closer reviews of transactional activity.

178 It is recognised that the most effective method of monitoring of accounts/business relationship is achieved through a combination of computerised and human manual solutions. A corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with customers, will form an effective monitoring method as a matter of course. Computerised approaches may include the setting of "floor levels" for monitoring by amount.

179 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 for the reasons of 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

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

181 Regardless of the source of "Hold Mail" business, evidence of identity of the account holder should be obtained by the SFI in accordance with paragraphs 49 (i) – (iii) and 50 (i) and (ii) of these Guidelines.

182 It is recommended that SFIs have controls in place for when existing accounts change status to "Hold Mail", 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.

183 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 of course 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.

184 Hold Mail" accounts should be annually monitored and reviewed. SFIs should establish procedures to conduct annual checks of the current permanent address of hold mail customers.

V MONEY TRANSMISSION BUSINESSES

185 The following guidance applies to persons other than banks 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.

186 In accordance with section 31(j)(v) of the FTRA, providers and their agents are covered by the definition of "financial institutions". Consequently, providers and their agents are expected to adhere to all of the requirements of the FTRA, the FTRR, the FIUA and subsidiary legislation made thereunder.

187 It is the responsibility of each MTB to have an AML/CFT programme in place comprising policies to prevent money laundering and terrorist financing. 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 programme;
- monitor its money transmission agents for compliance with its AML/CFT programme; and
- document the basis on which it is satisfied with its money transmission agents' compliance with the AML/CFT programme.

Where a MTB observes any non-compliance with its AML/CFT programme, it should document its findings and consider whether to take any remedial action, such as the termination of the agency agreement. The MTB should obtain approval from its senior

management on the proposed action to be taken, including any proposal not to take any action.

Vulnerability of MTBs to Money Laundering & Terrorist Financing

188 The fleeting relationship with its customers makes MTBs 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 repeatedly use different MTBs to transact business. The MTB is particularly vulnerable, given the high volume of cash handled on a daily basis and the ability to transmit funds instantly to any part of the globe.

189 While the international remittance system is typically used by expatriate workers to send a part of their earnings back home, it can also be used to transmit the illegal 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.

190 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

191 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.

Given the fleeting nature of the customer relationship, MTBs should obtain identification information where the customer, product or geography is deemed to be high risk.

Customer identification information should 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

192 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

193 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 attempting to hide the size of a large cash transaction by breaking it into multiple, smaller transactions by, for example, conducting the smaller transactions -

    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 usual activities of the customer.

- A business customer sends or receives money transfers to/from persons in other countries without an apparent business reason or gives a reason inconsistent with the customer's business.
- A business customer sends or receives money transfers to or from persons in other countries when the nature of the 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 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

194 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, 2015 ("the Wire Transfers Regulations").

195.1 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

195.2 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.

195.3 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.

195.4 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

195.4.1 SFIs that participate in the execution of wire transfers should monitor wire transfers to and from higher risk countries or jurisdictions, as well as transactions with higher risk countries or jurisdictions and suspend or reject 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.

195.4.2Where 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.

195.4.3Where there are positive hits arising from name screening checks, they should be escalated to the AML/CFT compliance function 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.

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

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

195.6 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 195.5(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 195.5(ii).

195.7 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.

195.8 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".

195.9 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.

195.10 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.

195.11 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

195.12 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 195.5. 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

195.13 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

195.14 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

195.15 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

195.15.1 As part of their internal controls, intermediary financial institutions should adoptrisk-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

195.16 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

195.17 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

195.18 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.

195.19 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 assessment;

(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.

195.20 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.

195.21 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.

195.22 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

195.23 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

195.24 As indicated in paragraph 195.23(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.

195.25 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

195.26 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

VII - RECORD KEEPING

196 Sections 23, 24 and 25 of the FTRA require financial institutions to retain records concerning customer identification and transactions for use as evidence in any investigation into money laundering or terrorist 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.

Often the only significant role a financial institution can play in a money laundering or terrorist financing investigation is through the provision of relevant records, particularly where the money launderer or terrorist financier has used a complex web of transactions specifically for the purpose of confusing the audit trail.

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

197 The records prepared and maintained by an 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 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

198 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.

199 Records relating to the verification of the identity of facility holders, 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.-

200 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.

201 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.

202 In the case of SFIs (being a company) that are liquidated and finally dissolved, the relevant records (both verification and transaction records), must be retained by the liquidator of the SFI for the balance of the prescribed period remaining at the date of dissolution.

203 The obligation to retain records also applies where an SFI verifies the identity of any person by confirming the existence of a facility provided by an eligible introducer financial institution. In this instance, the records that are retained must be such as are reasonably necessary to enable the FIU to readily identify, at any time, the other financial institution, the relevant facility and to confirm that the other financial institution has verified the person's identity.

204 Where a facility holder conducts a transaction through a facility provided by a financial institution, and in accordance with the provisions of section 9 of the FTRA, the financial institution verifies the identity of any non-facility holder in relation to that facility, the records generated by such verification must be kept by the financial institution for a period of not less than five years after the facility holder ceases to be a facility holder.

205 In relation to any other records relating to the verification of the identity of any person such records must be kept for a period of not less than five years after the verification was carried out.

Transaction Records

206 Transaction records must be kept for a minimum period of five (5) years after the transaction has been completed.

207 The investigating authorities need to be able to compile a satisfactory audit trail for suspected laundered money or terrorist financing and to be able to establish a financial profile of any suspect account/facility. For example, the following

information may be sought as part of an investigation into money laundering or terrorist financing:

(i) the identity of the beneficial owner of the account/facility and any intermediaries involved;

(ii) the volume of funds flowing through the account/facility; and

(iii) for selected transactions:

* the source of the funds (if known);
* the form in which the funds were offered or withdrawn, i.e., cash, cheques, etc.;
* the identity of the person undertaking the transaction;
* the destination of the funds; and
* the form of instruction and authority.

208 At a minimum therefore, the records relating to transactions which must be kept must include the following information:

- the nature of the transaction;
- details of the transaction including the amount of the transaction, and the currency in which it was denominated;
- the date on which the transaction was conducted;
- details of the parties to the transaction;
- where applicable, the facility through which the transaction was conducted, and any other facilities directly involved in the transaction; and
- reliable accounting records.

208.1 When providing trustee services, in addition to any other requirement to maintain accounting records required by any other law or under any other direction from the Central Bank, a SFI is required to maintain accounting records pertinent to its trusteeship and appropriate to the trust and trust property. The accounting records required to be kept should include related underlying documentation. Accounting records under these Guidelines are required to be kept for a minimum period of five years.

Records related to ongoing investigations and inquiries into suspicious or unusual activity

209 Records of suspicions which were raised internally with the MLRO but not disclosed to the authorities should be retained for at least five years from the date of the transaction. Records of suspicions which the authorities have advised are of no interest should be retained for a similar period.

Similarly, records of SFIs' findings of their enquiries into unusual activity, should be retained for a minimum of five years following the termination of the business relationship or after the date of the occasional transaction.

210 Section 28(3) of the FTRA provides that where the records relate to on-going investigations, they must be retained until it is confirmed that the case has been closed.

Format of Records

211 It is recognised that SFIs will find it necessary to rationalise their hard copy filing requirements. Most will have standard procedures which seek to reduce the volume and density of records which have to be stored, whilst still complying with statutory requirements. Retention may, therefore, be by way of original documents, stored on microfiche, computer disk or in other electronic form (see regulation 11 of the FTRR).

212 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

213 SFIs should appoint a MLRO to whom employees must report their knowledge or suspicions of customers who are engaged in money laundering or the financing of terrorism.

214 The type of person appointed as MLRO will depend upon the size of the SFI and the nature of its business, but he or she should be sufficiently senior to command the necessary authority.

215 The MLRO has significant responsibilities and is required to determine whether the information or other matters contained in the transaction report he or she has received gives rise to a knowledge or suspicion that a customer is engaged in money laundering or the financing of terrorism.

216 In making this judgment, the MLRO should have timely access to all other relevant information such as customer identification data and other CDD information transaction records available within an SFI concerning the person or business to which the initial report relates. 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 decides that the initial report gives rise to a knowledge or suspicion of money laundering or terrorist financing, then the MLRO must disclose information about the former to the FIU and about the latter to the Commissioner of Police.

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

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

IX - EDUCATION AND TRAINING

Requirements

219 SFIs must take appropriate measures to make employees aware of:

- policies and procedures put in place to detect and prevent money laundering and to counter the financing of terrorism including those for identification, record keeping, the detection of unusual and suspicious transactions and internal reporting; and
- the relevant legislation pertaining to AML/CFT, and to provide relevant employees with training in the recognition and handling of suspicious transactions.

The Need for Staff Awareness

220 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.

221 It is, therefore, important 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

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

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

224 Where SFIs observe unusual activity in relation to any client account they should question the customer concerned, even if this means asking "awkward" questions. Any failure by the customer to provide credible answers will almost always give grounds for 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 record their findings in writing of their enquiries into all unusual activity.

225 Where the staff member conducts enquiries and obtains what he considers to be a satisfactory explanation of the unusual transaction, or unusual pattern of transaction, he may conclude that there are no grounds for suspicion, and therefore take no further action as he is satisfied with matters. 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.

Reporting Procedures

226 The national reception point for disclosure of suspicious transaction reports is the Financial Intelligence Unit, 3rd Floor Norfolk House, Frederick Street, P.O. Box SB-50086, Nassau, The Bahamas, Telephone No. (242) 356-9808 or (242) 356-6327, Fax No. (242) 322-5551.

227 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

228 Timing and content of training for various sectors of staff will need to be adapted by individual institutions for their own needs. The Financial Intelligence (Transactions Reporting) Regulations, 2001 provide that, at least once per year, financial institutions shall 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 and terrorist 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. They should be made aware of 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 are dealing 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 be made aware of 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, and of the need for extra vigilance in these cases.

Branch staff should be trained to recognise that criminal money may not only be paid in or drawn out across branch counters but maybe transferred by other means. 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 in the above paragraph. In addition, further training should be provided in respect of the need to verify a customer's identity and on the business' own account opening and customer/client verification procedures. They should also be familiarised with the business' suspicious transaction reporting procedures.

(d) Administration/Operations Supervisors and Managers

A higher level of instruction covering all aspects of AML/CFT procedures should be provided to those with the responsibility for supervising or managing staff. This will 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; and, the requirements for verification of identity, the retention of records, and disclosure of suspicious transaction reports under the FIUA, 2000.

(e) Money Laundering Reporting Officer and Compliance Officer

In-depth training concerning all aspects of the legislation and internal policies will be required for the MLRO and Compliance Officer. In addition, the MLRO and Compliance Officer will require extensive initial and on-going instruction on the validation, investigation and reporting of suspicious transactions and on the feedback arrangements and on new trends and patterns of criminal activity.

229 It will also be necessary to make arrangements for refresher training at least annually to ensure that staff do not forget their responsibilities.

APPENDIX A

SUMMARY OF EXISTING BAHAMIAN LAW

The following summaries do not constitute a legal interpretation of the legislation referred to. SFIs should consult their professional advisers for appropriate legal advice when and where necessary.

The laws of The Bahamas specifically concerning money laundering and terrorist financing and the requirements that financial institutions know their customers are found in the following legislation:

- the Proceeds of Crime Act, 2000, Ch. 93,
- the Anti-Terrorism Act, 2004, Act No. 25 of 2004,
- the Financial Transactions Reporting Act, 2000, Ch. 368, the Financial Transactions
- Reporting Regulations, 2000, Ch. 368,
- the Financial Transactions Reporting (Wire Transfers) Regulations, 2015
- the Financial Intelligence Unit Act, 2000, Ch. 367,
- the Financial Intelligence (Transactions Reporting) Regulations, 2001, Ch. 367

I PROCEEDS OF CRIME ACT, 2000

Confiscation Orders

Section 9 of the Act provides that any person convicted of one or more drug trafficking offences committed after the commencement of this Act shall be liable to have a confiscation order made against him relating to the proceeds of drug trafficking.

For the purposes of this Act a person has benefited from drug trafficking if that person, at any time after the commencement of the Act or for the period of six years prior to proceedings being instituted against him, received any payment or other reward in connection with drug trafficking carried on by him or another person.

Section 10 of the Act allows for a confiscation order to be made against any person convicted of one or more relevant offences committed after the coming into operation of the Act. The "relevant offences" are those offences described in the Schedule to the Act as follows:

(1) an offence under the Prevention of Bribery Act, Chapter 81 of the Statute Laws of The Bahamas, 1987 Edition;

(2) an offence under section 40, 41, or 42 of this Act (Money Laundering);

(3) an offence which may be tried on information in The Bahamas other than a drug trafficking offence;

(4) an offence committed anywhere that if it had occurred in The Bahamas, would constitute an offence in The Bahamas as set out in the Schedule to the Act, and

(5) an offence under the Anti-Terrorism Act, 2004.

The court must first determine whether such a person has benefited from the principal offence or offences for which he is to be sentenced and secondly from any relevant offences which the court will be taking into consideration in determining his sentence for the principal offence.

For the purposes of the Act, a person benefits from a relevant offence if:

(a) he obtains property as a result of or in connection with its commission and his benefit is the value of such property; and

(b) he derives a pecuniary advantage as a result of or in connection with its commission and his benefit is the amount of or the value of the pecuniary advantage of an offence. In these circumstances, he is to be treated as if he had obtained instead a sum of money equal to the value of the pecuniary advantage.

Section 11 of the Act provides that for the purpose of determining whether a person has benefited from drug trafficking and for determining the value of his proceeds of drug trafficking the court must assume, unless the contrary is shown:

(a) that any property shown to the court –

(i) to have been held by the defendant; or

(ii) to have been transferred to him at any time since the beginning of the period of six years ending when the proceeding was instituted against him, was received by him as a payment or reward in connection with drug trafficking carried on by him;

(a) that any expenditure of his since the beginning of that period was met out of payments received by him in connection with drug trafficking carried on by him;

(c) that, for the purpose of valuing any property received or assumed to have been received by him at any time as such a reward; he received the property free of other interests in it.

Section 15 of the Act provides that a third party who has an interest in any property that is the subject of a confiscation order may apply to the court for an order either before the order is made or otherwise with the leave of the court, declaring the nature, extent and value of his interest.

Charging Orders

Section 27 of the Act provides that a court may make a charging order imposing a charge on property specified in the order for securing the payment of money to the Crown. An application for a charging order may be made only by the Police or the Attorney-General. Property which may be the subject of a charging order includes, inter alia, any monies held by or deposited with a bank or other financial institution, the stock of any body corporate, and a debt instrument.

Production Orders

Section 35 of the Act empowers a Stipendiary and Circuit Magistrate upon application by a Police officer of or above the rank of Inspector, to make a production order where the Magistrate is satisfied that there is reasonable cause to believe that any person is in possession of material in respect of which a drug trafficking offence or relevant offence has been committed. The order would require a person to produce relevant material in his possession for the Police.

A production order shall not extend to items subject to legal privilege. However, it shall have effect notwithstanding any obligation as to confidentiality or other restriction upon the disclosure of information imposed by the Banks and Trust Companies Regulation Act, 2000, the Central Bank of The Bahamas Act, 2000, any other statute or otherwise and shall not give rise to any civil liability. Where a production order requires information which is restricted under the Banks and Trust Companies Regulation Act, 2000 or the Central Bank of The Bahamas Act, 2000, application for an order shall be made ex-parte to a judge in chambers.

A production order may be made in relation to material in the possession of a Government Department (excluding the Financial Intelligence Unit).

Monitoring Orders

Section 39 of the Act provides that a police officer may apply to a Judge in Chambers for a monitoring order directed to any police officer of or above the rank of Inspector, directing a bank or trust company to give the officer information obtained by the institution in respect of transactions conducted through an account or accounts held by a person under investigation, with the institution.

The monitoring order is to be made where the Judge is satisfied by evidence on oath that there is reasonable cause to believe that a person has committed or is about to commit a drug trafficking offence or a relevant offence; or was involved in the commission or is about to become involved in the commission of such an offence; or has benefited directly or indirectly

from the commission of such an offence. The disclosure of information in these circumstances is not to be treated as a breach of any restriction upon disclosure of information imposed by the Banks and Trust Companies Regulation Act, 2000, The Central Bank of The Bahamas Act, 2000, any other statute or otherwise. Additionally, such disclosure shall not give rise to any civil liability.

The Offence of Money Laundering

Section 40 of the Act provides that a person is guilty of the offence of money laundering if he uses, transfers, sends or delivers to any person or place any property which, in whole or in part directly or indirectly represents proceeds of criminal conduct; or disposes of, converts, alters or otherwise deals with that property in any manner and by any means with the intent to conceal or disguise such property.

A person is also guilty of money laundering if he knows, suspects or has reasonable grounds to suspect that any property in whole or in part directly or indirectly represents another person's proceeds of criminal conduct and he uses, transfers, sends or delivers to any person or place that property; or disposes of or otherwise deals with in any manner by any means that property, with the intent to conceal or disguise the property.

Section 41 of the Act provides inter alia that it is an offence for a person to assist another to retain or live off the proceeds of criminal conduct knowing, suspecting, or having reasonable grounds to suspect that the other person is or has been engaged in or has benefited from criminal conduct.

It is a defence for a person to prove that he or she did not know, suspect or have reasonable grounds to suspect that -

(a) the arrangement in question related to any person's proceeds of criminal conduct; or

(b) the arrangement facilitated the retention or control of any property by or on behalf of the suspected person; or

(c) by arrangement any property was used as mentioned in section 41(1)(b).

Further, it is a defence for a person to prove that he intended to disclose to a police officer a suspicion, belief or matter that any funds or property are derived from or used in connection with criminal conduct; but there is a reasonable excuse for failing to do so as prescribed in subsection (2)(b) of the Act.

Section 42 of the Act provides that a person is guilty of an offence if he knows, suspects or has reasonable grounds to suspect that any property in whole or in part directly or indirectly represents, another person's proceeds of criminal conduct, and he acquires or uses that property or has possession of it.

Penalty for failing to disclose suspicious transaction

Section 43 of the Act makes it an offence for a person who knows suspects or has reasonable grounds to suspect that another person is engaged in money laundering, which relates to any proceeds of drug trafficking or any relevant offence, to fail to disclose this to the Financial Intelligence Unit or to a police officer.

A person is also guilty of an offence where the information, or other matter, on which his knowledge or suspicion is based came to his attention in the course of his trade, profession, business or employment and he fails to disclose the information or other matter to a police officer as soon as is reasonably practicable after it comes to his attention.

It is a defence to prove that the person had a reasonable excuse for not disclosing the information or other matter in question. It should be noted that a person is not required to disclose information or to provide a document which is subject to legal professional privilege. However, a counsel and attorney-at-law may be required to provide the name and address of his client or principal.

Offence of disclosing information prejudicial to an investigation ("Tipping Off")

Section 44 of the Act makes it an offence to disclose information that is likely to prejudice an investigation if the person knows, suspects or has reasonable grounds to suspect that an investigation into money laundering is being, or is about to be, conducted or if he knows, suspects or has reasonable grounds for suspecting that a disclosure has been made under section 41, 42 or 43.

It is a defence to prove that the person did not know or suspect that the disclosure was likely to prejudice the investigation or that he had lawful authority or reasonable excuse for making the disclosure.

Penalty for offences under sections 43 and 44

A person guilty of an offence under section 43 to 44 shall be liable on summary conviction, to imprisonment for three years or to a fine of $50,000.00 or both; or on conviction on information, to imprisonment for ten years or an unlimited fine or both.

Penalty for money laundering

Section 45 of the Act provides that a person guilty of an offence under section 40, 41 or 42 shall be liable on summary conviction to imprisonment for five years or a fine of $100,000.00 or both; and on conviction on information, to imprisonment for twenty years or an unlimited fine or both.

External Confiscation Orders

Section 49 of the Act provides that the Minister responsible for the Police may, by order direct in relation to a country outside The Bahamas, designated by the order, that subject to such modifications as may be specified, the Act shall apply to external confiscation orders and to proceedings which have been or are to be instituted in the designated country and may result in an external confiscation order being made there.

Section 50 of the Act provides that upon the application made by or on behalf of the government of a country designated by an Order of the Minister under section 49, the Supreme Court may register an external confiscation order made in a designated country, if satisfied of certain conditions, and such registered order shall be enforceable in The Bahamas in the same manner as a confiscation order made by a court in The Bahamas. (Countries have been designated by Statutory Instrument No. 6 of 2001, which includes most of the major countries).

Offences by a body corporate

Section 54 of the Act provides that where a body corporate is found guilty of an offence under this Act and the offence is proven to have been committed with the consent or connivance of any director, manager, secretary or other similar officer of the body corporate or any person who was purporting to act in any such capacity he, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

II. ANTI-TERRORISM ACT, 2004

The Offence of Terrorism

Section 3(1) of the Act provides inter alia that a person who in or outside The Bahamas carries out any of the following acts is guilty of the offence of terrorism:

(a) an act that constitutes an offence under or defined in any of the treaties listed in the First Schedule of the Act; or

(b) any other act that is intended to intimidate the public or to compel a government or an international organization to do or refrain from doing any act, and that is intended to cause –

(i) death or serious bodily harm to a person;

(ii) a serious risk to public health or safety;

(iii) damage to property; or

(iv) which causes interference with or disruption of an essential service, facility or system.

Section 3(2) of the Act provides that it is an offence for a person to aid, abet, counsel, procure, incite or solicit the commission of the offence of terrorism or to conspire with another or others to commit this offence.

Order in respect of listed entities

Section 4 of the Act authorizes the Attorney General to apply to the Supreme Court for a declaration that an entity is a listed entity (entities designated as terrorist entities by the United Nations Security Council). On an application by the Attorney General, the Court must be satisfied that the entity is in fact a listed entity and that the Attorney General has reasonable grounds to believe that the entity:

(a) has knowingly committed or participated in the commission of a terrorism offence; or

(b) is knowingly acting on behalf of, or at the discretion of or in association with, a listed entity.

Providing or collecting funds for criminal purposes

Section 5(1) of the Act provides inter alia that it is an offence for a person to provide or collect funds or provide financial services or make such services available to persons if it is known or intended that the funds or services are to be used to carry out terrorist activities. For an act to constitute an offence under section 5(1), it is not necessary to prove that the funds or the financial services were used to carry out the offence.

Section 5(3) of the Act provides inter alia that it is an offence for a person to aid, abet, counsel, procure, incite or solicit the commission of the offence of terrorism or to conspire with another or others to commit this offence.

Liability of a legal entity

Section 6 provides inter alia that where an offence under section 3 or 5 is committed by a person responsible for the management or control of an entity located or registered in The Bahamas or in any other way organized under the laws of The Bahamas while acting in that capacity, that entity is guilty of an offence.

Investigation

Section 7(1) of the Act provides inter alia that a person who has reasonable grounds to suspect that funds or financial services are related to or are to be used to facilitate an offence under this Act, have a duty to report the matter to the Commissioner of Police.

Freezing of funds

Section 9 of the Act authorizes the Attorney General to apply to the Court for an order freezing the funds in possession of or under the control of a terrorist. On application, the Court must be satisfied that:

(a) the person has been charged or is about to be charged with an offence of terrorism;

(b) the person has been declared a listed entity under the Act; and

(c) a request has been made by the appropriate authority of another State in accordance with section 17, in respect of a person –

(i) who has been charged or is about to be charged with an offence under the Act; or

(ii) where there is reasonable suspicion that the person has committed an offence under the Act.

Forfeiture order

Section 10(1) of the Act provides that where a person is convicted of an offence under section 3 or 5, the Attorney General may apply to the Court for a forfeiture order against the funds that are the subject of an offence.

Section 10(2) of the Act provides that the Court may upon application by the Attorney General, forfeit any funds of or in the possession or under the control of any person who is convicted of an offence of terrorism or any funds of that person that are the subject of a freezing order, unless it is proved that the funds did not derive from the commission by that person of an offence under section 3 or 5.

Sharing of forfeited funds

Section 11(1) of the Act provides that the Government of The Bahamas may, pursuant to any forfeiture agreement with any State, share with that State on a reciprocal basis, the funds derived from forfeiture pursuant to this Act.

III. THE FINANCIAL TRANSACTIONS REPORTING ACT, 2000

The Financial Transactions Reporting Act, 2000, ("the Act") mandates that financial institutions as defined in section 3 of the Act, verify the identity of their customers in the circumstances set out in the Act.

The occasions when an SFI may obtain and rely upon written confirmation of identity from another financial institution are set out in Section IV of these Guidelines _Reliance on third parties to conduct KYC on Customers'.

Section 3 of the Act defines "financial institution".

The Act makes it mandatory for financial institutions to verify the identity of the following persons:

Persons who wish to become facility holders

Section 6 of the Act provides that the identity of such persons must be verified before they become facility holders (see section 6(1) and 6(2)).

Existing facility holders whose identities are doubtful

Where during the course of a business relationship the financial institution has reason to doubt the identity of an existing facility holder, the financial institution shall seek to verify the identity of such facility holder (see section 6(4)).

Occasional Transactions

Section 7 of the Act provides for the mandatory verification by a financial institution of the identity of a person who conducts an occasional transaction by, through or with a financial institution in any case where:

(a) the amount of cash involved in the transaction exceeds the prescribed amount of $15,000.00 (this verification must take place before the transaction is conducted) and in these circumstances, the financial institution shall also ask the person who is conducting or who has conducted the transaction whether or not the transaction is or was being conducted on behalf of any other person (see section 7(1)(a), 7(4)(a) and 7(5)); or

(b) one or more other occasional transactions have been or are being conducted by that person or any other person through the financial institution;

(c) the financial institution has reasonable grounds to believe that the transactions have been or are being structured so that the amount of cash involved in the transaction do not exceed the prescribed amount of $15,000.00; and

(d) the total amount of cash involved in those transactions exceeds the prescribed amount (see section 7(1)(b)).

In determining whether or not any transactions are or have been structured to avoid the application of section 7(1)(a), the financial institution shall consider the following factors:

(a) the time frame within which the transactions are conducted; and

(b) whether or not the parties to the transactions are the same person, or are associated in any way (see section 7(3)).

In any case where the conditions referred to in (b), (c) or (d) above apply, verification must be made as soon as practicable after the conditions specified in section 7(1)(b) are satisfied in respect of that transaction (see section 7(4)(b)).

Section 8 of the Act provides for the mandatory verification by a financial institution of the identity of the following persons:

- a person on whose behalf an occasional transaction is being conducted by, through or with a financial institution in circumstances where the cash involved in the transaction exceeds the prescribed amount and the financial institution has reasonable grounds to believe that the person conducting the transaction does so on behalf of any other person or persons. Such verification must take place before the transaction is completed (see section 8(1) and 8(4));

- a person on whose behalf an occasional transaction has been conducted**,** in circumstances where the financial institution has reasonable grounds to believe, after the occasional transaction has been conducted, that the person who conducted the transaction was acting on behalf of another person or persons; and

- a person of whom it is believed that one or more occasional transactions are or have been conducted on his behalf in circumstances where the transactions have been or are being structured to avoid the application of section 8(1) and the total amount of cash involved in those transactions exceed the prescribed amount (see section 8(2)).

In determining whether or not any transactions are or have been structured to avoid the application of section 8(1), the financial institution shall consider the following factors:

(a) the time frame within which the transactions are conducted; and

(b) whether or not the parties to the transactions are the same person(s), or are associated in any way (see section 8(3)).

Section 9 of the Act provides for the mandatory verification of the identity of the persons on whose behalf a transaction is being or has been conducted by a facility holder through a facility provided by a financial institution where:

- **in the case of a single transaction**

(a) the amount of cash involved in the transaction exceeds the prescribed amount of $15,000.00; and,

(b) the financial institution has reasonable grounds to believe that the person is conducting the transaction on behalf of others.

Such verification must take place before the transaction is conducted (see section 9(1) and 9(4)).

- **in the case where the facility holder has also conducted or is conducting one or more other transactions through that facility**

(a) the financial institution has reasonable grounds to believe that the facility holder is conducting the transaction on behalf of others;

(b) the financial institution has reasonable grounds to believe that the transactions have been structured to avoid the application of the mandatory verification procedure required by the Act; and

(c) the total amount of cash involved in the transactions exceeds the prescribed amount.

Such verification must take place as soon as practicable after these conditions are satisfied (see section 9(2) and 9(5)).

In determining whether or not any transactions are or have been structured to avoid the application of section 9(1), the financial institution shall consider the following factors:

(a) the time frame within which the transactions are conducted;

(b) whether or not the parties to the transactions are the same person(s) or are associated in any way (see section 9(3)).

Section 10A of the Act provides for the mandatory verification by a financial institution of the identity of any person (whether as a facility holder or not) whom they know, suspect or have reasonable grounds to suspect is conducting or proposes to conduct a transaction which involves the proceeds or criminal conduct as defined in the Proceeds of Crime Act, 2000 or is an attempt to avoid the enforcement of the Proceeds of Crime Act, 2000.

Section 11 of the Act provides that where verification of identity is required by the Act, it shall be done by means of such documentary or other evidence as is reasonably capable of establishing the identity of a person, including official documents and structural information in the case of corporate entities.

A financial institution may rely in whole or in part on evidence used by it on an earlier occasion to verify that person's identity, if the institution has reasonable grounds to believe that the evidence is still reasonably capable of establishing the identity of that person.

Such verification may be accepted from a foreign financial institution subject to the agreement of the financial institution's Supervisory Authority and if the foreign financial institution is located in a country mentioned in the First Schedule.

Section 12 of the Act provides that an offence is committed where a financial institution:

(a) in contravention of section 6(2), permits a person to become a facility holder in relation to any facility without having first verified the identity of that person;

(b) in contravention of section 7(4)(a), permits any person to conduct an occasional transaction in excess of $15,000.00 without first having verified the identity of that person;

(c) in contravention of section 7(4)(b), fails to verify the identity of a person conducting an occasional transaction as soon as practicable after the conditions set out in section 7(1)(b) have been satisfied in respect of that transaction;

(d) in contravention of section 8(4) fails to verify the identity of a person on whose behalf an occasional transaction in excess of $15,000.00 is being or has been conducted;

(e) in contravention of section 8(5), fails to undertake the verification required by section 8(2) in relation to persons conducting an occasional transaction in excess of 15,000.00 in circumstances where it reasonably appears that the transaction is being conducted on behalf of any other person or persons and that the transactions are or have been structured to avoid verification of identity;

(f) in contravention of section 9(4), fails, before a transaction is conducted, to verify the identity of a person on whose behalf a facility holder is conducting a transaction in excess of $15,000.00 that where it has reasonable grounds to believe the circumstances set out in section 9(1) exist; and

(g) in contravention of section 9(5), fails to undertake the verification required by section 9(2);

A financial institution which commits any of the foregoing offences is liable on summary conviction to a fine not exceeding:

(a) in the case of an individual, $20,000.00;
(b) in the case of a body corporate, $100,000.00.

Suspicious Transactions

Section 14 of the Act makes it mandatory for a financial institution to report to the Financial Intelligence Unit any transaction conducted by, through or with a financial institution or any proposed transaction (whether or not the transaction involves funds) where the financial institution knows, suspects or has reasonable grounds to suspect that the transaction or proposed transaction involves proceeds of criminal conduct as defined in the Proceeds of Crime Act, 2000, or any offence under the Proceeds of Crime Act, 2000, or an attempt to avoid the enforcement of any provision of the Proceeds of Crime Act, 2000.

The financial institution must as soon as practicable after forming a suspicion, report the transaction to the Financial Intelligence Unit.

Every suspicious transaction report shall be in writing, and shall contain the details set out in the Second Schedule to the Act.

A report must also contain the grounds on which the financial institution holds a suspicion.

A report may be forwarded to the Financial Intelligence Unit by way of facsimile transmission, or by other means (including without limitation, electronic mail or other similar means of communication) as may be agreed from time to time between the Financial Intelligence Unit and the financial institution concerned.

Oral Reports

Section 14 of the Act also provides that where the urgency of the situation so requires, a suspicious transaction report may be made orally to the Financial Intelligence Unit; however, the financial institution shall, as soon as practicable, forward to the Financial Intelligence Unit a suspicious transaction report that complies with the requirements of the Act.

Penalty for failing to report suspicious transactions

A person who contravenes the provisions of section 14(1) shall be liable on summary conviction to a fine not exceeding – in the case of an individual, $20,000.00 and, in the case of a body corporate, $100,000.00 (see section 20(2)).

It is a defence for a person to prove that he took all reasonable steps to ensure that he complied with the provisions of section 14(1) or that, in the circumstances of the particular case, he could not reasonably have been expected to ensure that he complied with the provision (see section 21).

Auditors to report suspicious transactions

Section 15 of the Act provides that an auditor is under a duty to report suspicious transactions to any member of the Financial Intelligence Unit, where in the course of

carrying out the duties of his occupation as an auditor, he has reasonable grounds to suspect, in relation to any transaction that the transaction is or may be relevant to the Proceeds of Crime Act, 2000. No civil, criminal or disciplinary proceedings shall lie against an auditor who makes a suspicious transaction report pursuant to section 15.

Protection of persons reporting suspicious transactions

Section 16 of the Act provides protection from civil, criminal or disciplinary proceedings to persons who report suspicious transactions in accordance with the provisions of the Act.

Legal Professional Privilege

Section 17 of the Act provides that the mandatory reporting provisions of the Act do not apply to the disclosure of privileged information by a Counsel and Attorney, except however, that where the information consists wholly or partly of, or relates wholly or partly to, the receipts, payments, income, expenditure or financial transactions of a specified person (whether a counsel and attorney, his or her client or any other person), the information shall not be a privileged communication if it is contained in or comprises the whole or part of any book, account, statement or other record prepared or kept by the counsel and attorney in connection with a client's account of the counsel and attorney.

Persons to whom suspicious transaction reports may be disclosed

Section 18 of the Act restricts the persons to whom a financial institution may disclose that they have made or are contemplating making a suspicious transaction report. Apart from the Financial Intelligence Unit, reports may be disclosed only to the financial institution's supervisory authority; the Commissioner of Police or a member of the Police authorized by the Commissioner to receive the information; an officer or employee or agent of the financial institution, for any purpose connected with that person's duties; a counsel and attorney for the purpose of obtaining legal advice or representation in relation to the matter; and, the Central Bank of The Bahamas for the purpose of assisting the Central Bank of The Bahamas to carry out its function under the Central Bank of The Bahamas Act, 2000.

Section 20(7) of the Act provides that a person who knowingly contravenes section 18(1) to (3) is liable upon summary conviction to:

(a) in the case of an individual, a fine not exceeding $5,000.00 or to imprisonment for a term not exceeding 6 months;

(b) in the case of body corporate, a fine not exceeding $20,000.00.

Protection of Identity

Section 19 of the Act provides inter alia that no person shall be required to disclose, in any judicial proceeding, any suspicious transaction report, or any information the disclosure of

which will identify, or is reasonably likely to identify, the officer, employee or agent of a financial institution who has handled a transaction in respect of which a suspicious transaction report was made, or who has prepared a suspicious transaction report, or who has made a suspicious transaction report, unless the Judge or, as the case requires, the person presiding at the proceeding is satisfied that the disclosure of the information is necessary in the interests of justice.

Penalty for making false statements and for "Tipping Off"

Section 20 of the Act provides that:

(1) it is an offence for a person, in making a suspicious transaction report, to make a statement which they know to be false or misleading in a material particular or to omit from any statement any matter or thing without which the person knows that the statement is false or misleading in a material particular. A person who commits this offence is liable on information to a fine not exceeding $10,000.00 (see section 20(3));

(2) a person who contravenes sections 18(1) to (3), for the purpose of obtaining, directly or indirectly, an advantage or a pecuniary gain for that person or any other person, or with intent to prejudice any investigation into the commission or possible commission of a money laundering offence, commits an offence and is liable on summary conviction to a term of imprisonment not exceeding two years (see section 20(4));

(3) an officer, employee or agent of a financial institution who, having become aware, in the course of that person's duties as such an officer or employee or agent, that any investigation into any transaction or proposed transaction that is the subject of a suspicious transaction report is being, or may be, conducted by the Police:

(a) knowing that he or she is not legally authorised to disclose the information; and

(b) either:

(i) for the purpose of obtaining, directly or indirectly, an advantage or a pecuniary gain for that person or any other person; or

(ii) with intent to prejudice any investigation into the commission or possible commission of a money laundering offence, discloses that information to any other person is guilty of an offence (see section 20(5)).

Penalty

Summary conviction for these offences carries a term of imprisonment not exceeding two years.

Application of information contained in a suspicious transaction report

Section 22 of the Act provides that information contained in a suspicious transaction report is deemed to be obtained for certain limited purposes such as, inter alia: the detection, investigation, and prosecution of offences against the Act; the enforcement of the Proceeds of Crime Act, 2000; or, the detection, investigation and prosecution of any relevant offence (within the meaning of the Proceeds of Crime Act, 2000), in any case where that offence may reasonably give rise to, or form the basis of, any proceedings under the Proceeds of Crime Act, 2000.

Retention of Records

Section 23 of the Act provides that financial institutions are obligated to retain transaction records for a period of not less than five years after the completion of a transaction. The records that are to be retained are those that are reasonably necessary to enable the Financial Intelligence Unit to re-construct a transaction.

The records should include information concerning the nature of the transaction; the amount of the transaction, and the currency in which it was denominated; the date on which the transaction was conducted; the parties to the transaction; and, where applicable, each facility (whether or not provided by the financial institution) directly involved in the transaction.

Section 24 of the Act provides that where a financial institution is required by section 6, 7, 8, 9, or 11 of the Act, to verify the identity of any person, the financial institution 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 Financial Intelligence Unit (see section 24(1)).

The obligation to retain records also applies where a financial institution verifies the identity of any person by confirming the existence of a facility provided by another financial institution. In this instance, the records that are retained should be such as are reasonably necessary to enable the Financial Intelligence Unit to readily identify, at any time, the identity of the other financial institution, the identity of the relevant facility and the identity confirmation of the person (see section 24(3)).

Such reports may comprise a copy of the evidence so used or, where it is not practicable to retain that evidence, such information as is reasonable necessary to enable that evidence to be obtained.

Records relating to the verification of the identity of persons making a request to become facility holders, and to the identity of existing facility holders must be retained for five years after a person ceases to be a facility holder (see section 24(4)).

Records relating to the verification of the identity of any non-facility holder in relation to a facility, where the verification was carried out pursuant to section 9, with respect to a person who is such a facility holder, shall be kept by a financial institution for a period of not less than five years.

In relation to any other person, records relating to the verification of the identity of any person shall be kept for a period of not less than five years after the verification was carried out.

Section 25 of the Act directs financial institutions to keep records which are prescribed by any regulations made under this Act, pursuant to section 42, and to retain them for any prescribed period.

Section 26 of the Act provides that records must be kept either in written form in the English language or so as to enable the records to be readily accessible and readily convertible into written form in the English language.

Section 27 of the Act provides that records need not be retained where a company has been liquidated and finally dissolved or a partnership has been dissolved provided that the liquidator of the company shall maintain relevant records for the balance of the prescribed period remaining at the date of dissolution.

Section 28 of the Act provides that a financial institution shall ensure the destruction of records retained for the purposes of Part IV of the Act, as soon as practicable after the expiry of any retention period provided by Part IV of the Act.

Destruction of records is not required where there is a lawful reason for retaining them. There is a lawful reason for retaining a record if the retention of a record is necessary:

(a) in order to comply with the requirements of any other written law;

(b) to enable any financial institution to carry on its business; or

(c) for the purposes of the detection, investigation or prosecution of any offence.

Section 29 of the Act provides that other laws which require any financial institution to keep or retain any record, are not affected by Part IV of the Act.

Section 30 of the Act provides that it is an offence for a financial institution to fail, without reasonable excuse, to retain or properly keep records sufficient to satisfy the requirements of this section.

A person guilty of an offence under this section is liable on summary conviction to a fine not exceeding in the case of an individual, $20,000.00 and in the case of a body corporate, $100,000.0.

IV. FINANCIAL TRANSACTIONS REPORTING REGULATIONS, 2000

These Regulations prescribe the information which a financial institution is required to obtain to verify the identity of any person.

Regulation 2 provides that for the purposes of Part II of the Financial Transactions Reporting Act, 2000, the prescribed amount shall be the sum of $15,000.00.

Regulation 3 sets out the information that financial institutions must obtain when they seek to verify the identity of individual customers namely the full and correct name of the individual, their address, date and place of birth, and the purpose of the account (facility) and the nature of the business relationship. In addition, regulation 3 introduces a risk based approach to customer due diligence and provides financial institutions with guidance on the type of information and documentation they may rely upon (apart from the required information) when verifying an individual customer's identity and includes information such as the source of funds, telephone and fax numbers(if any), occupation and name of employer (if self-employed, the nature of the self-employment), copy of the relevant pages of passport, drivers licence, voter's card, national identity card or such other identification document bearing a photographic likeness of the person as is reasonably capable of establishing the identity of the person, or such documentary or other evidence as is reasonably capable of establishing the identity of that individual.

Regulations 4 and 5 set out the minimum mandatory information which financial institutions must obtain when verifying the identities of corporate entities, partnerships and other unincorporated businesses. Like regulation 3 these regulations adopt a risk based approach to verifying the identities of corporate entities, whether incorporated in The Bahamas or elsewhere (Regulation 4), partnerships and other unincorporated businesses (Regulation 5) and provide financial institutions with guidance on the type of information and documentation they may rely upon when verifying these entities.

Regulation 5A provides for exemption from verification procedures by those customers with a Bahamian dollar facility of or below $15,000.00 and certain financial institutions and other agencies or bodies save where there is a suspicion of money laundering or terrorist financing.

Regulation 7 provides that where any request is made to a financial institution, by telephone, internet, or written communication for a person, corporate entity or partnership to become a facility holder, the financial institution should (subject to certain exceptions) obtain the information set out in regulation 3 to 5 as appropriate.

Regulation 7A requires financial institutions to verify the identities of the beneficial owners of all facilities. In the case of corporate entities the obligation to verify beneficial owner identity is limited to those beneficial owners having a controlling interest in the corporate entity. For the purposes of these Guidelines, the Central Bank defines "controlling interest" as an interest of ten percent or more in a corporate entity's voting shares.

Regulation 9 requires further verification of customer identity (after the establishment of the business relationship), if there is a material change in the way a customer's facility is operated. Although material change is not defined in the regulation, the Central Bank is of the view that a material change is a change which is inconsistent with a facility holder's account profile. Financial institutions are required to monitor facility holders for consistency with the facility holder's stated account purposes during the business relationship.

Regulation 10 provides that where a facility holder closes one facility and opens another facility, the financial institution shall confirm the identity of the facility holder and obtain any additional information with respect to the facility holder and all records relating to the existing account shall be transferred to the new facility and retained for the relevant period.

Regulation 11 provides that records required by section 23, 24, or 25 of the Act to be kept by any financial institution may be stored on microfiche, computer disk or in other electronic form.

V. FINANCIAL TRANSACTIONS REPORTING (WIRE TRANSFERS) REGULATIONS, 2015

Regulation 3 requires financial institutions that initiate wire transfers on behalf of payers (originating financial institutions), to verify the payer's identity and obtain the verification documentation in accordance with the Financial Transaction Reporting Act, 2000 and the Financial Transactions Reporting Regulations, 2000 before conducting a transfer of funds.

Regulation 4 provides that the following 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:

(a) name of the payer and payee;

(c) account number of the payer and payee, or if no account is used, a unique transaction identifier; and

(d) address, or date and place of birth of the payer, or national identity number, or customer identification number.

Regulation 5 provides that for batch file transfers comprised of individual funds transfers of $1,000 or more from a single payer to a beneficiary financial institution outside The Bahamas, the individual transfers within the batch file need carry only the payer's account number or a unique transaction identifier, provided that the batch file itself contains complete payer and payee information as indicated in Regulation 4(a) and (b).

Regulation 6 sets out the information that must accompany domestic funds transfers. Where the originating and beneficiary financial institutions are both located within The Bahamas, wire transfers need be accompanied only by the payer's account number or a unique transaction identifier which permits the transaction to be traced back to the payer. However, if requested by the beneficiary financial institution or the intermediary

financial institution (i.e. the financial institution other than originating or beneficiary financial institution that participates in the execution of wire transfers), complete payer information must be provided by the originating financial institution within three business days of such request.

Regulation 7 provides that where the beneficial financial institution of the payee is situated outside of The Bahamas, transfers of funds of less than one thousand dollars must be accompanied by the information required under sub-paragraphs (i) and (ii) of paragraph (a) and paragraph (b) of Regulation 4.

Regulations 8 outlines the record keeping requirements for wire transfers. An originating financial institution must keep a record of any information on the payer and the payee obtained under regulations 3 and 4 for a period of five years.

Regulation 9 provides that where an originating financial institution is unable to comply with the requirements outlined in Regulations 3 to 7, or if the financial institution has any suspicion of money laundering or terrorism financing, then the originating financial institution shall not execute the wire transfer.

Regulation 10 refers to the measures that the intermediary financial institution should take in instances where technical limitations exist.

Regulation 11 provides that when payer and payee information is missing, intermediary financial institutions shall take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers.

Regulation 12 provides that intermediary financial institutions shall adopt risk-based policies and procedures that will enable them to determine when to execute, reject of suspend wire transfers that are lacking the complete payer and payee information, as well as the appropriate follow-up action to take in these cases.

Regulation 13 provides that every beneficiary financial institution must take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required payer and payee information.

Regulation 14 provides for cross-border wire transfers of BSD 1,000 or more originating outside The Bahamas, beneficiary financial institutions must verify the identity of the payees (where such verification was not previously done).

Regulation 15 provides that every beneficiary financial institution 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.

Regulation 16 provides failure to comply with the Regulations is an offence punishable on summary conviction by a fine not exceeding $2,000. As an alternative to prosecution, a financial institution's Supervisory Authority may impose a fine not exceeding $2,000.

Regulation 17 provides for exemption from the requirements of the Regulations, 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 a 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.

Regulation 18 provides that financial institutions that control both the originating and the beneficiary side of a wire transfer must take into account all information from the originating and the beneficiary financial institutions to determine whether to file a suspicious transaction report ("STR"). Financial institutions must file a STR in any country affected by the suspicious wire transfer and make relevant transaction information available to the appropriate authorities.

VI. FINANCIAL INTELLIGENCE UNIT ACT, 2000

By virtue of section 3, the Financial Intelligence Unit Act, 2000 (No. 39 of 2000) ("the Act") establishes the Financial Intelligence Unit of The Bahamas (the "FIU") giving it wide powers to enter into contracts and to do all such things necessary for the purpose of its functions.

Section 4(1) of the Act empowers the FIU to act as the agency responsible for receiving, analysing, obtaining and disseminating information which relates or may relate to the proceeds of offences under the Proceeds of Crime Act, 2000.

Sections 4(2)(a)-(i) of the Act provide that the FIU may:

- receive all disclosures of information required to be made pursuant to the Proceeds of Crime Act, 2000;
- receive information from any Foreign Financial Intelligence Unit;
- order in writing any person to refrain from completing any transaction up to a maximum period of seventy-two hours;
- freeze a person's bank account for a maximum period of five days upon receipt of a request from a foreign FIU or law enforcement authority including the Commissioner of Police of The Bahamas;
- require the production of information (except information subject to legal professional privilege) which it considers relevant to fulfill its functions;

- share information relating to the commission of an offence under the Proceeds of Crime Act, 2000 with the local law enforcement agency including the Commissioner of Police;
- provide information to foreign FIU's relating to the commission of an offence under the Proceeds of Crime Act, 2000;
- enter into any agreement or arrangement in writing with a foreign FIU for the discharge or performance of the functions of the FIU;
- inform the public and financial and business entities of their obligations under measures that have been or might be taken to detect, prevent and deter the commission of offences under the Proceeds of Crime Act, 2000;
- retain a record of all information it receives for a minimum of five years after the information is received.

Section 4(3) of the Act provides that it is an offence for a person to fail or refuse to provide this information and on summary conviction a person is liable to a fine not exceeding $50,000.00 or to imprisonment for a term not exceeding two years or to both such fine and imprisonment.

Section 6 of the Act provides that no order for the provision of information, documents or evidence may be issued in respect of the FIU or against the Minister, Director, Officers or personnel of the FIU or any person engaged pursuant to this Act.

Section 7 of the Act provides that no action shall lie against the Minister, Director, Officers or personnel of the FIU or any person acting under the direction of the Director, for anything done or omitted to be done in good faith and in the administration or discharge of any functions, duties or powers under this Act.

No Civil or Criminal Liability

Section 8 of the Act provides that no proceedings for breach of banking or professional confidentiality may be instituted against any person or against directors of a financial or business entity who transmit information or submit reports in good faith in pursuance of this Act or the Proceeds of Crime Act, 2000.

Section 8(2) of the Act further provides that no civil or criminal liability action may be brought nor any professional sanction taken against any person or against directors or employees of a financial or business entity who in good faith transmit information or submit reports to the FIU.

Section 9 of the Act prohibits disclosure of information obtained by any person as a result of his connection with the Financial Intelligence Unit, unless this is required or permitted under this Act or any written law.

Any person who contravenes this provision commits an offence and shall be liable on summary conviction to a fine not exceeding $10,000.00 or to a term of imprisonment not exceeding one year or to both such fine and imprisonment.

VII. FINANCIAL INTELLIGENCE (TRANSACTIONS REPORTING) REGULATIONS, 2001

The Financial Intelligence (Transactions Reporting) Regulations, 2001 (Statutory Instrument No. 7 of 2001) require financial institutions to establish and maintain the following procedures and practices:

Regulation 3 provides that a financial institution shall establish and maintain identification procedures in compliance with Part II of the Financial Transactions Reporting Act, 2000 and the provisions of the Financial Transactions Reporting Regulations, 2000.

Regulation 4 provides that a financial institution shall establish and maintain record-keeping procedures in compliance with Part IV of the Financial Transactions Reporting Act, 2000 and the provisions of the Financial Transactions Reporting Regulations, 2000.

Regulation 5 provides, inter alia, that a financial institution shall institute and maintain internal reporting procedures which include provision for the appointment of a MLRO and a Compliance Officer. These roles may be performed by the same person.

The MLRO must be registered with the FIU. Financial Institutions must institute and maintain internal reporting procedures which include provisions requiring the MLRO to disclose to the FIU, relevant agency or to a police officer the information or other matter contained in a suspicious transaction report, where the MLRO knows, suspects or has reasonable grounds to suspect a person is engaged in money laundering.

Regulation 6 places an obligation on financial institutions to provide appropriate training from time to time for all relevant employees, at least once per year. Financial Institutions are required to take appropriate measures from time to time to make all relevant employees aware of the provisions of the Financial Intelligence Unit Act, 2000 and the Regulations made thereunder, the Financial Transactions Reporting Act, 2000, the Financial and Corporate Service Providers Act, 2000, the Proceeds of Crime Act, 2000, and any other statutory provision relating to money laundering. Employees must also be made aware of the procedures maintained by the financial institution in compliance with the duties imposed under these Regulations. Training must be given to all new relevant employees as soon as practicable after their appointment.

Regulation 8 provides that failure to comply with the requirements of these Regulations or any guidelines issued pursuant to section 15 of the Financial Intelligence Unit Act, or with codes of practice or other instructions issued by a relevant agency, is an offence punishable on summary conviction by a fine of $10,000.00 and on conviction on information by a fine of $50,000.00 for a first offence and by a fine of $100,000.00 for a second or subsequent offence.

It is a defence to prove that a financial institution took all reasonable steps and exercised due diligence to comply with the requirements of the Regulations, guidelines, codes or instructions.

APPENDIX B

1. IDENTIFICATION PROCEDURES

Information on the status of sanctions can be obtained from websites such as http://www.fco.gov.uk

Other useful websites include:
http://www.un.org/en/
https://www.fbi.gov/
https://www.treasury.gov/Pages/default.aspx
http://www.bankofengland.co.uk/
http://www.osfi-bsif.gc.ca/swppws/default.html

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")

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

(b) 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 recent 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.

(c) 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.

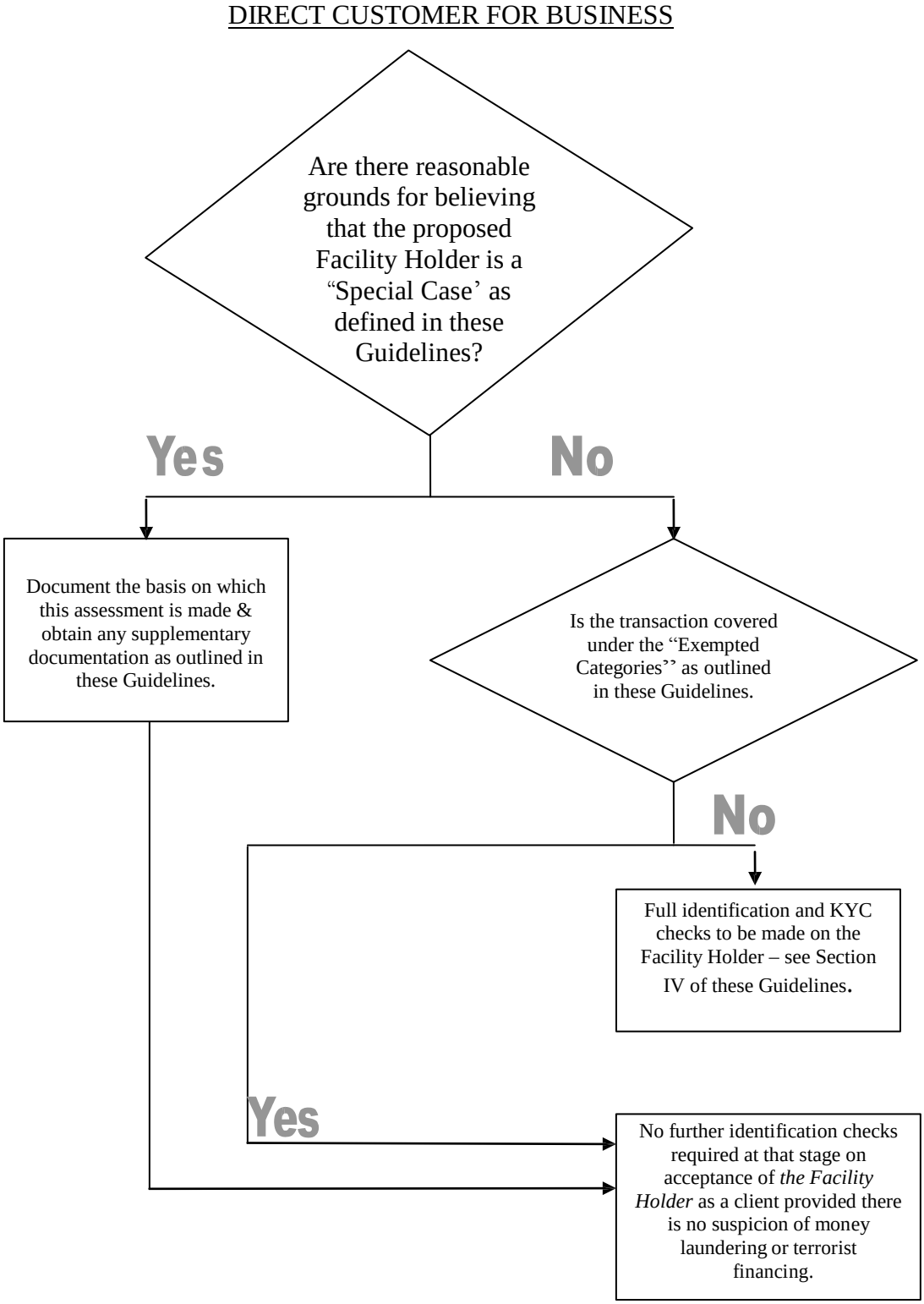
4. HIGH RISK COUNTRIES

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 C

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.



COUNTRIES LISTED IN THE FIRST SCHEDULE OF THE FINANCIAL TRANSACTIONS REPORTING ACT, 2000[1]

Financial institutions in the countries and territories listed below are recognised and may be treated as institutions which exercises functions equivalent to the corresponding financial institution in The Bahamas and which adhere to a standard of anti-money laundering and anti-terrorist financing regime which is at least equivalent to that of The Bahamas.

Countries-

Australia
Austria
Bahrain
Barbados
Belgium
Bermuda
Brazil
British Virgin Islands
Canada
Cayman Islands
Channel Islands
Chile
Denmark
Finland
France
Germany
Gibraltar
Greece
Hong Kong SAR
India
Israel
Ireland
Isle of Man
Italy
Japan
Liechtenstein
Luxembourg
Malta
Mexico
Netherlands
New Zealand
Norway
Panama
Portugal
Singapore
South Africa
Spain
Sweden
Switzerland
United Kingdom
United States

[1] The Minister of Finance may by order add to, or delete from, the list of countries mentioned in this Schedule.

APPENDIX E

DEFINITION OF FINANCIAL INSTITUTION

Section 3 of the FTRA as amended by the Financial Transactions Reporting (Amendment) Act, 2015, defines a financial institution as:

(a) a bank or trust company, being a bank or trust company licensed under the Banks and Trust Companies Regulation Act;

(b) a company carrying on life assurance business as defined in section2 of the Insurance Act or insurance business as defined in section 2 of the External Insurance Act;

(c) a co-operative credit union registered under The Bahamas Cooperative Credit Unions Act;

(d) a friendly society enrolled under the Friendly Societies Act;

(e) the holder of a gaming licence, proxy gaming licence, mobile gaming licence, restricted interactive gaming house operator licence under the Gaming Act 2014 Act;

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

(g) a real estate broker, but only to the extent that the real estate broker receives funds in the course of the person's business for the purpose of settling real estate transactions;

(h) a trustee or administration manager or investment manager of a superannuation scheme;

(i) an investment fund administrator of an investment fund within the meaning of the Investment Funds Act, 2003;

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

  (i) borrowing or lending or investing money;

  (ii) administering or managing funds on behalf of other persons;

  (ii) acting as trustee in respect of funds of other persons;

  (iv) dealing in life assurance policies;

  (v) providing financial services that involve the transfer or exchange of funds, 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;

(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;

(m) a financial and corporate service provider licensed under the Financial and Corporate Service Providers Act;

(n) any person whose business or any part of whose business consists of any of the following—

(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

(ii) lending of money 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.