<table>
<thead>
<tr>
<th>SECTION. #</th>
<th>DESCRIPTION</th>
<th>PARAGRAPH</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECTION I</td>
<td>SCOPE AND PURPOSE OF GUIDELINES</td>
<td>1 - 4</td>
</tr>
<tr>
<td>SECTION II</td>
<td>LEGISLATIVE FRAMEWORK</td>
<td>5</td>
</tr>
<tr>
<td>SECTION III</td>
<td>EXPLANATORY FOREWORD</td>
<td>6 - 10</td>
</tr>
<tr>
<td>SECTION IV</td>
<td>BACKGROUND</td>
<td>11 – 25</td>
</tr>
<tr>
<td></td>
<td>What is Money Laundering?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What is Terrorism and Financing of Terrorist Activities?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What is Financing Proliferation of Weapons of Mass Destruction?</td>
<td></td>
</tr>
<tr>
<td>SECTION V</td>
<td>BUSINESSES COVERED BY THESE GUIDELINES</td>
<td>26 – 27</td>
</tr>
<tr>
<td>SECTION VI</td>
<td>KNOW YOUR CUSTOMER AND CUSTOMER DUE DILIGENCE</td>
<td>28 – 34</td>
</tr>
<tr>
<td>SECTION VII</td>
<td>WHAT BAHAMIAN LAW REQUIRES</td>
<td>35 – 46</td>
</tr>
<tr>
<td></td>
<td>Proceeds of Crime Act 2000, As Amended</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Financial Transactions Reporting Act, 2000, As Amended</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Financial Transactions Reporting Regulations, 2000, As Amended</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Financial Intelligence Unit Act, 2000, As Amended</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Financial Intelligence (Transactions Reporting) Regulations, 2001, As Amended</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anti-Terrorism Act, 2004</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Financial Transactions Reporting (Wire Transfers) Regulations, 2009</td>
<td></td>
</tr>
<tr>
<td>SECTION VIII</td>
<td>THE ROLE OF THE MONEY LAUNDERING REPORTING OFFICER</td>
<td>47 - 74</td>
</tr>
<tr>
<td>SECTION IX</td>
<td>WHAT IS A “SUSPICIOUS TRANSACTION?”</td>
<td>75 - 82</td>
</tr>
<tr>
<td>SECTION X</td>
<td>REPORTING OF SUSPICION</td>
<td>83 - 98</td>
</tr>
<tr>
<td>SECTION XI</td>
<td>MONITORING METHODS AND PROCEDURES</td>
<td>99 113</td>
</tr>
<tr>
<td>SECTION XII</td>
<td>REPORTING TO THE FINANCIAL INTELLIGENCE UNIT (THE “FIU”)</td>
<td>114 - 128</td>
</tr>
<tr>
<td>SECTION XIII</td>
<td>REPORTING PROCEDURES</td>
<td>129-137</td>
</tr>
<tr>
<td>SECTION XIV</td>
<td>MONEY TRANSMISSION BUSINESSES</td>
<td>138-151</td>
</tr>
<tr>
<td>SECTION XV</td>
<td>ELECTRONIC PAYMENTS TRANSFERS</td>
<td>152-178</td>
</tr>
<tr>
<td>SECTION XVI</td>
<td>CASH COURIERS</td>
<td>179-183</td>
</tr>
<tr>
<td>SECTION XVII</td>
<td>USE OF THE FINANCIAL SYSTEM</td>
<td>184</td>
</tr>
<tr>
<td>SECTION XVIII</td>
<td>SOURCES AND USE OF FUNDS</td>
<td>185-190</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Pages</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>XIX</td>
<td>Record Keeping</td>
<td>191-196</td>
</tr>
<tr>
<td>XX</td>
<td>Significant Local Trends with Implications for Financial Services</td>
<td>197-257</td>
</tr>
<tr>
<td></td>
<td>Cash For Gold</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Copper and Scrap metals</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Counterfeit Products and Smuggling</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cyber Crime</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firearms Trafficking (Pending)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fraud</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trafficking in Persons</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lotteries</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-Profit Organizations (Pending)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scams</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tax Evasion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Weapons of Mass Destruction</td>
<td></td>
</tr>
<tr>
<td>XXI</td>
<td>Money Laundering and Financing of Terrorism Offences, Penalties and Defense</td>
<td>258-271</td>
</tr>
<tr>
<td></td>
<td>Proceeds of Crime Act, 2000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Financial Transactions Reporting Act, 2000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anti-Terrorism Act, 2004</td>
<td></td>
</tr>
<tr>
<td>XXII</td>
<td>Examples of Terrorism Financing</td>
<td>272</td>
</tr>
</tbody>
</table>

**Appendices**

<table>
<thead>
<tr>
<th>Letter</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>International Conventions</td>
<td>65-78</td>
</tr>
<tr>
<td>B</td>
<td>Money Laundering and Terrorism Financing “Red Flags”</td>
<td>79-85</td>
</tr>
<tr>
<td>C</td>
<td>Suspicious Transactions Indicators</td>
<td>86-98</td>
</tr>
<tr>
<td>D</td>
<td>Collection of Sanitized Cases Related to Terrorism Financing</td>
<td>99</td>
</tr>
<tr>
<td>E</td>
<td>Money Laundering Schemes Uncovered Worldwide</td>
<td>100</td>
</tr>
<tr>
<td>F</td>
<td>Examples of Suspicious Transactions</td>
<td>101-108</td>
</tr>
<tr>
<td>G</td>
<td>New Typologies By Sector</td>
<td>109-118</td>
</tr>
<tr>
<td>H</td>
<td>Suspicious Transactions Report Template</td>
<td>119-124</td>
</tr>
<tr>
<td>I</td>
<td>Acknowledgement and Production Letters from the FIU</td>
<td>125-127</td>
</tr>
<tr>
<td>J</td>
<td>Sources Utilized to Prepare the Guidelines</td>
<td>128-129</td>
</tr>
<tr>
<td>K</td>
<td>Glossary</td>
<td>130-131</td>
</tr>
</tbody>
</table>

**Suspicious Transactions Guidelines for Financial**
I - SCOPE AND PURPOSE

1._ These Guidelines replace those, which were initially issued by the Financial Intelligence Unit (the “FIU”) on 19th March 2007. The Guidelines have been updated in light of amendments to The Bahamas’ Anti-Money Laundering and Anti-Terrorism Financing Legislation which have occurred between January 2007 and July 2013. Further, the Guidelines have been prepared in consultation with local regulators of financial services in The Bahamas, and those financial institutions and industry organizations that expressed an interest in being consulted in the course of the development of same. Further, the FIU also utilized materials from a number of external sources in preparing these Guidelines, as indicated in Appendix J, and is grateful for such assistance.

2._ The Guidelines apply to all financial institutions in The Bahamas, as defined in Section 3 of the Financial Transactions Reporting Act, 2000 (FTRA), as amended. The Guidelines remain narrowly focused on ‘suspicious transactions’ but also seek to address, from a reporting perspective, a number to related issues given new trends emerging locally and globally including global concerns regarding the financing of the proliferation of weapons of mass destructions. Financial institutions are reminded to be guided by Guidelines, if any, issued by their respective regulatory authorities where there is overlap on any related issues.

3._ Further, the Guidelines have been issued in recognition that the financial services sector in The Bahamas, as elsewhere, is exposed to the risks of assisting in laundering the proceeds of criminal conduct and involvement in the financing of terrorism. Accordingly, they have been produced to accord with evolving international standards, as are currently reflected in the financial laws and business practices of The Bahamas.

4._ Since the late 1980s, both the Basel Committee (Basel) and the Financial Action Task Force (FATF) have issued international standards for financial services which have been adopted by many countries, including the Commonwealth of The Bahamas, and implemented via legislation in a global effort to combat money laundering and financing of terrorism.

II - LEGISLATIVE FRAMEWORK

BAHAMIAN ANTI-MONEY LAUNDERING AND ANTI-TERRORISM LEGISLATIVE FRAMEWORK
The laws of The Bahamas, specifically concerning money laundering and terrorist financing is contained in the following legislation:

- the Proceeds of Crime Act, 2000 (as amended) (POCA);
- the Anti-Terrorism Act, 2004 (as amended) (ATA);
- 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, 2009;
- the Financial Intelligence Unit Act, 2000 (as amended) (FIUA); and
- the Financial Intelligence (Transactions Reporting) Regulations, 2001 (as amended).

A summary of the aforementioned statutes is provided in Section VII.

III - EXPLANATORY FOREWORD

6. The Bahamian Parliament approved the Financial Intelligence Unit Act, 2000 (the “Act”) in December 2000. The Act, as amended, established the FIU as an independent, administrative agency with authority to:

(a) receive all disclosures of information made pursuant to the Proceeds of Crime Act, 2000 (POCA), as amended, including information from a Foreign Financial Intelligence Unit (FFIU);
(b) order the freezing of transactions on accounts for a period not exceeding 72 hours;
(c) at the request of a Foreign Financial Intelligence Unit or law enforcement authority, including the Commissioner of Police of The Royal Bahamas Police Force, order the freezing of account transactions for a further five days; and
(d) to require the production of such information, excluding information which may be the subject of legal professional privilege, that the FIU considers relevant to its functions.

7. Under the Egmont Group’s classification of FIUs, The Bahamas’ FIU is an ‘Administrative Model FIU.’ The Administrative Model is a centralized, independent, administrative authority, which receives and processes information from the financial sector and transmits disclosures to judicial or law enforcement authorities for prosecution. It functions as a “buffer” between the financial and the law enforcement communities.

8. The Financial Intelligence Unit of The Bahamas is empowered by Section 15 of the Financial Intelligence Unit Act, 2000, Chapter 367, as amended, to issue ‘Suspicious Transactions Guidelines’ for the prevention of money laundering and terrorism financing, from time to time, in respect of each category of financial institution to which the Financial Transactions
Reporting Act, 2000, Chapter 368, as amended, and the Anti-Terrorism Act, 2004, Chapter 107, as amended, apply, and to amend or revoke such guidelines from time to time. These guidelines are formulated to provide a practical interpretation of the provisions of the various amendments to the relevant legislation and to give typologies of such transactions.

9._ **The Proceeds of Crime Act, 2000, as amended**, makes provision generally for:

(a) dealing with the proceeds of criminal conduct, including drug trafficking and money laundering by means of, inter alia, seizure and detention of the proceeds of crime and forfeiture and confiscation orders;
(b) suspicion of the offences of money laundering;
(c) penalties for “tipping off”;
(d) enforcement of local and external confiscation orders and, in the case of external confiscation orders, registration of such orders by the Supreme Court; and
(e) for reporting of suspicious transactions.

10._ **The Anti-Terrorism Act, 2004, as amended**, makes provision, inter alia, generally for:

(a) the definition of a “terrorist act”;
(b) the creation of the offence of terrorism where any person outside of The Bahamas commits a terrorist act;
(c) the making of an Order in respect of an entity included on a List of the United Nations Security Counsel or where the Attorney General has reasonable grounds to suspect the entity has committed a terrorist offence. It gives effect to an Order of the Security Counsel of the United Nations designating a listed entity;
(d) the offence of providing or collecting funds for criminal purposes; for the investigation of terrorist offences; for the extradition or prosecution of persons who have committed offences under the Act or who are alleged to have committed offences under the Act; for the conditions of transfer of persons who are serving a sentence of imprisonment in the territory of one state and whose presence is requested in another state for purposes of identification, testimony or otherwise providing assistance in obtaining evidence for the investigation or prosecution purposes; and
(e) the necessary consequential amendment to the Proceeds of Crime Act 2000 and the Financial Intelligence Unit Act, 2000.
IV - BACKGROUND

WHAT IS MONEY LAUNDERING?

11._ The expression “money laundering” covers all procedures to conceal the origins of criminal proceeds so that they appear to have originated from a legitimate source (see Sections 40, 41 and 42 of the Proceeds of Crime Act 2000, as amended). This gives rise to three features common to persons engaged in criminal conduct, namely that they seek: -
- to conceal the true ownership and origin of criminal proceeds;
- to maintain control over them; and
- to change their form.

Money laundering also includes the hiding of the origin of legally acquired money where it will be used to finance criminal activities.

12._ There are three stages of laundering, which broadly speaking, occur in sequence but often overlap.

12.1 I. **Placement** is the physical disposal of criminal proceeds. In the case of many serious crimes, the proceeds take the form of cash, which the criminal wishes to place in the financial system. Placement may be achieved by a wide variety of means according to the opportunity afforded to and the ingenuity of the criminal, his advisers and network. Typically, it may include: -
- placing of cash on deposit at a bank (often intermingled with a legitimate credit to obscure the audit trail), thus converting cash into a readily recoverable debt; or
- physically moving cash between jurisdictions; or
- making loans in cash to businesses which seem to be legitimate or are connected with legitimate businesses, thus also converting cash into debt; or
- purchasing high-value goods for personal use or expensive presents to reward existing or potential colleagues; or
- purchasing the services of high-value individuals; or
- purchasing negotiable assets in one-off transactions; or
- placing cash in the client account of a professional intermediary.

12.2 II. **Layering** is the separation of criminal proceeds from their source by the creation of complex layers of financial transactions designed to disguise the audit trail and to provide the appearance of legitimacy. Again, this may be achieved by a wide variety of means according to the opportunity afforded to, and the ingenuity of, the criminal, his advisers and network. Typically, it may include:
- rapid switches of funds between banks and/or jurisdictions; or
• use of cash deposits as collateral security in support of legitimate transactions; or
• switching cash through a network of legitimate businesses and “shell” companies across several jurisdictions; or
• re-sale of goods/assets.

12.3 **Integration** is the stage in which criminal proceeds are treated as legitimate. If layering has succeeded, integration places the criminal proceeds back into the economy in such a way that they appear to be legitimate funds or assets.

13._ The Bahamas’ good reputation makes it potentially vulnerable as a staging post for funds at the layering stage and the integration stage. Other international financial centers face a similar problem. Therefore, financial services businesses should recognize that, The Bahamas could be targeted by money launderers, terrorists and those seeking to place their proceeds of crime, and that, financial institutions are the gate keepers for protecting the reputation and integrity of The Bahamian financial services industry.

14._ The criminal remains relatively safe from detection systems while criminal proceeds are not moving through these stages and remain static. Certain points of vulnerability have been identified in the stages of laundering which the launderer finds difficult to avoid and where his activities are therefore more susceptible to recognition, in particular:
• cross-border flows of cash;
• entry of cash into the financial system;
• transfers within and from the financial system;
• acquisition of investments and other assets;
• incorporation of companies; and
• formation of trusts.

15._ Accordingly, detection systems require financial services businesses and their key staff to be most vigilant at these points along the audit trail where the criminal is most actively seeking to launder, i.e. to misrepresent the source of criminal proceeds.

16._ However, in an increasingly cashless society, there should be good reason, and sufficient explanation, for anyone wishing to deposit or withdraw large quantities of cash. Whilst there is no mandatory cash transaction reporting legislation in place, financial services businesses should question any such significant transactions and, in the absence of an adequate explanation, consider them suspicious and report them to the FIU using the report form found at Appendix H attached hereto.

17._ Financial services businesses are reminded that, especially in the context of local criminality and terrorism, although cash transactions could be relatively low in value, this does not detract from the need to consider them carefully and, if suspicious, report them to the FIU.
18. **Appendix E** contains examples of various schemes of laundering detected by Foreign FIUs and other law enforcement authorities. One of the recurring features of many such schemes is the urgency with which, after a brief “cleansing,” the assets are often reinvested in new criminal activity.

### WHAT IS TERRORISM AND THE FINANCING OF TERRORIST ACTIVITY?

19. **The Anti-Terrorism Act, 2004** defines the offence of terrorism and criminalizes the financing of terrorism. It applies to actions, persons and property both inside and outside The Bahamas. 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.

20. Terrorists often control funds from a variety of sources around the world and employ increasingly sophisticated techniques to move these funds between jurisdictions. In doing so, they require the services of skilled financial professionals such as accountants, bankers and lawyers. Persons employed in these areas of financial services should be vigilant and try to stay abreast of the latest trends utilized by terrorists to legitimize their funds, so as to avoid their services from being targeted.

21. There may be a considerable overlap between the movement of terrorist funds and the laundering of criminal assets; terrorist groups often have links with other criminal activities. There are, however, two major differences between the use of terrorist and other criminal funds: -

- often only small amounts are required to commit a terrorist act. This makes terrorist funds harder to detect; and
- terrorism can be funded from legitimately obtained income such as donations – it will often not be clear at what stage legitimate earnings become terrorist assets.

“Red Flags” or “Indicators” of activities related to financing of terrorism can be found in **Appendix B and Appendix C** of these Guidelines.

22. The risk of terrorist funding entering The Bahamas’ financial system can be reduced, if robust anti-money laundering procedures are followed, particularly in respect of verification procedures. Terrorist funding can come from any country. Financial institutions should assess which countries pose a high risk and should conduct careful scrutiny of transactions from jurisdictions known to be a source of terrorist financing.
WHAT IS FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION (WMDs)?

23._ Proliferation finance refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

24._ Countries are required to implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.

25._ In response to the United Nations’ Resolution on preventing financing for proliferation of WMDs, The Bahamas enacted the International Obligations (Economic and Ancillary Measures) Act, 1993. This Act provides the basis for imposition of economic sanctions and taking of ancillary measures to give effect to the international obligations of The Bahamas.

V – BUSINESSES COVERED BY THESE GUIDELINES

26. Businesses covered by these Guidelines are highlighted in Section 3 of the FTRA, as amended, which 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, 2000;
(b) a company carrying on life assurance business as defined in section 2 of the Insurance Act or insurance as defined under section 2 of the External Insurance Act;
(c) a co-operative society registered under the Co-operative Societies Act;
(d) a friendly society enrolled under the Friendly Societies Act;
(e) a licensed casino operator within the meaning of the Lotteries and Gaming 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 that 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 or operator 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,
   iii. 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 corporate and financial services provider’s license:
   i. for the purpose 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 services providers license;

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

27. The Courts, in determining if the financial institution has satisfactory internal procedures within the organization, shall have regard to any relevant Guidelines issued by the Financial Intelligent Unit and the relevant regulatory authority on the matter.

VI - KNOW YOUR CUSTOMER AND CUSTOMER DUE DILIGENCE
The term “Know Your Customer” (“KYC”) has been in use since the 1980s. Increasingly the term “Customer Due Diligence” (“CDD”), drawn from the Basel Committee on Banking Supervision paper of October 2001 “Customer Due Diligence for Banks”, is also used. CDD is mandated in Regulation 9 of the Financial Transactions Reporting Regulations, 2000. Essentially, the term CDD is being used to represent the same concept as “KYC” as reflected throughout the Guidelines. CDD measures involve:

(a) Identifying a customer and verifying a customer's identity using reliable, independent source documents, data or information;
(b) Identifying the beneficial ownership and control of the customer and taking reasonable measures to verify the identity of the beneficial owners and controllers such that a financial service business is satisfied that it knows who the beneficial owners and controllers are;
(c) Obtaining information on the nature of the customer's business and the customer's economic circumstances;
(d) Obtaining information on the purpose and intended nature of the business relationship;
(e) Obtaining information on the type, volume and value of the activity that can be expected within the relationship;
(f) Obtaining information on the source of funds and, subject to the risk assessment, obtaining information on the source of wealth;
(g) Monitoring activity and transactions undertaken within the relationship to ensure that the activity or transaction being conducted is consistent with the financial institution's knowledge of the customer; and
(h) Keeping the information relevant and up to date.

Sound CDD procedures are vital for all financial institutions because they:

(i) Help protect the financial institution and the integrity of The Bahamas’ financial sector by reducing the likelihood of the licensee becoming a vehicle for, or victim of, financial crime;
(j) Assist law enforcement by providing available information on customers or activities, funds and transactions being investigated;
(k) Constitute an essential part of sound risk management e.g. by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management; and
(l) Help to guard against identity theft.

Inadequacy or absent satisfactory CDD standards and controls can subject a licensee to serious customer and counterparty risks, especially reputational, operational, legal and concentration risks, which can result in significant financial cost to the business.
30._ CDD information is also a vital tool for employees in recognizing whether there are grounds for knowledge or suspicion of money laundering or where there are reasonable grounds to suspect terrorist financing. The information is also essential for the MLRO in assessing whether an internal report has foundation. It is only through knowledge of what constitutes normal activity for a customer that unusual activity can be recognized and, from the unusual incident that suspicious transactions or activity can be determined.

31. In relation to CDD, the FIU believes that to properly understand and manage the money laundering and terrorist financing risk (and other risks) that a customer may represent, it is prudent practice for financial institutions to be clear about the risk that individual customers or categories of customers represent. The criteria used in assessing customer risk will vary from financial institutions to financial institutions, based on each institution’s operations.

32._ Financial institutions therefore should have clear, documented customer acceptance policies and procedures which are based on their assessment of risk.

33. Financial institutions should apply a graduated customer acceptance policy which requires more extensive CDD procedures to be undertaken on customers who represent higher risk. Where an applicant for business poses a higher risk of money laundering or terrorist financing, financial institutions must undertake enhanced CDD procedures. Licensees should give particular attention to the following business relations and transactions:

(a) where the customer has not been physically present for identification purposes;
(b) correspondent banking;
(c) a business relationship or occasional transaction with a Politically Exposed Person (PEP);
(d) business relations and transactions with persons from or in countries and jurisdictions known to have inadequate AML/CFT;
(e) corporate clients who are able to issue bearer shares or bearer instruments.

34._ CDD requirements apply at the outset of a customer relationship or one-off transaction. They also apply, in relation to existing and continuing business relationships, when there is/are:

(a) A transaction that is suspected may be related to money laundering or terrorist financing;
(b) A pattern of behavior that causes a financial institution to know or suspect that the behavior is or may be related to money laundering or terrorist financing;
(c) Transactions or patterns of transactions that are complex or unusually large and which have no apparent economic or visible lawful purpose;
(d) The financial institution becomes aware of anything which causes it to doubt the identity of the person who, in relation to the formation of the business relationship, was the applicant for business;
(e) The financial institution becomes aware of anything which causes it to doubt the veracity or adequacy of CDD information and documentation already produced;
(f) A suspicion of money laundering or terrorist financing in respect of a person for whom identification evidence is not already held;
(g) A change in identification information of a customer;
(h) A change in underlying principals or third parties on whose behalf a customer acts;
(i) A change in the beneficial ownership and / or control of a customer;
(j) An absence of meaningful originator information on wire transfers;
(k) In respect of wire transfers, where a one-off payment in excess of $1,000.00 is to be made at the request of a non-account holding customer.

VII - WHAT THE BAHAMIAN LAW REQUIRES

35. The Bahamian law relating to money laundering and terrorism financing is contained in the following legislation:
   • The Proceeds of Crime Act, 2000 (as amended);
   • The Financial Transactions Reporting Act, 2000 (as amended);
   • The Financial Transactions Reporting Regulations, 2000 (as amended);
   • The Financial Intelligence Unit Act, 2000 (as amended);
   • The Financial Intelligence (Transactions Reporting) Regulations, 2001 (as amended);
   • The Anti-Terrorism Act, 2004 ; and

36. The Proceeds of Crime Act, 2000, as Amended:
   This Act criminalizes money laundering related to the proceeds of drug trafficking and other criminal conduct. The Act also provides for the confiscation of the proceeds of drug trafficking or any relevant offence as described in the Schedule to the Act; the enforcement of Confiscation Orders and investigations into drug trafficking, ancillary offences related to drug trafficking and all other relevant offences.

37. The law requires financial institutions and persons to inform the Financial Intelligence Unit, or a Police officer authorized to receive this information of any suspicious transactions. The Act provides immunity to such persons from legal action by clients aggrieved by the breach of confidentiality. It should be noted that the reporting of suspicious transactions is mandatory and a person who fails to report a suspicious transaction is liable to
prosecution.

The Financial Transactions Reporting Act, 2000, as Amended:
38. The Financial Transactions Reporting Act, 2000, imposes mandatory obligations on financial institutions to verify the identity of existing and prospective facility holders and persons engaging in occasional transactions; to maintain verification and transaction records for prescribed periods; and to report suspicious transactions, which involve the proceeds of criminal conduct as defined by the Proceeds of Crime Act 2000, to the Financial Intelligence Unit.

The Financial Transactions Reporting Regulations, 2000, as Amended:
39. The Financial Transactions Reporting Regulations, 2000, inter alia, sets out the evidence that financial institutions must obtain in satisfaction of any obligation to verify the identity of a client or customer.

The Financial Intelligence Unit Act, 2000, as Amended
40. The Financial Intelligence Unit Act, 2000 established the Financial Intelligence Unit of The Bahamas, as the Agency responsible for obtaining, receiving, analyzing and disseminating information, which relates to or may relate to offences under the Proceeds of Crime Act, 2000 and the Anti-Terrorism Act, 2004.

The Financial Intelligence (Transactions Reporting) Regulations, 2001, as Amended:
41. The Financial Intelligence (Transactions Reporting) Regulations, 2001, require financial institutions to establish and maintain identification, record-keeping, and internal reporting procedures, including the appointment of a Money Laundering Reporting Officer (MLRO). These Regulations also require financial institutions to provide appropriate training for relevant employees to make them aware of the statutory provisions relating to money laundering.

The Anti-Terrorism Act, 2004
42. The Anti-Terrorism Act, 2004 criminalizes terrorist financing. The Act provides that, any person who in or outside of The Bahamas directly or indirectly, unlawfully and willfully provides or collects funds or provides financial services or makes such services available to persons with the knowledge that the funds or services are to be used to carry out any act that contravenes the various Treaties listed in the First Schedule, or any other Act, with the intent to intimidate the public, causes bodily harm/injury or property damage, is guilty of an offense under the Act and is liable on conviction to imprisonment for a term of twenty five years. Any person who
suspects that funds or financial services are to be used for such purposes has a duty to report such matters to the Financial Intelligence Unit.

**Financial Transactions Reporting (Wire Transfers) Regulations, 2009**

43. The Financial Transactions Reporting (Wire Transfers) Regulations 2009 mandates that all financial institutions involved in the process of handling wire transfers for $1,000.00 or more, to recipients within or outside the Bahamas, must ensure that all identifying information on the payer, i.e. name, address, date/place of birth, account number, etc, is attached to the wire transfer in its initial stage by the initiating financial institution and remains with the wire transfer through the entire process until received by the payee at the beneficiary financial institution. Where such information is absent or incomplete, the intermediary or beneficiary financial institution can insist on receipt of the missing information from the remitting financial institution within three days by alternate means if necessary by mutual agreement.

44. Financial institutions are required to implement a ‘risk based’ approach for dealing with wire transfers which lack complete information on the payer. If warranted, the financial institution must file a suspicious transaction report with the FIU. Financial institutions are required to retain records of the payer’s identification and details of the wire transfer itself for a period of five years.

45. Transactions made within The Bahamas involving credit cards, debit cards, direct debits, payments to public authorities, cash withdrawals from one’s own account and transactions between financial institutions are exempt from the regulations.

46. 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.

**VIII - THE ROLE OF THE MONEY LAUNDERING REPORTING OFFICER**

47. The principal objective of the MLRO is to act as the focal point within a financial institution for the oversight of all activity relating to the prevention and detection of money laundering and terrorist financing. The responsibilities of the MLRO will normally include:

(a) undertaking the internal review of all suspicions in light of all available relevant information and determining whether or not such suspicions have substance and require disclosure to the FIU;

(b) maintaining all related records;
(c) giving guidance on how to avoid tipping off the customer if any disclosure is made and managing any resulting constructive trust scenarios;
(d) providing support and guidance to the Board and senior management to ensure that money laundering and terrorist financing risks are adequately managed;
(e) liaising with the FIU and participating in any other third party enquiries in relation to money laundering or terrorist financing prevention and detection, investigation or compliance; and
(f) providing reports and other information to senior management.

48. After the financial institution has identified a suitable candidate for the position of MLRO and he/she is approved by the relevant regulator the financial institution, must ensure that the MLRO is immediately registered with the FIU.

49. Each financial institution will have its own pre-requisites for the MLRO, and the type of person appointed as Money Laundering Reporting Officer (MLRO) will depend upon the size of the financial institution and the nature of its business. However, he or she should be sufficiently senior and possesses the requisite authority to take independent decisions on whether or not to file a Suspicious Transaction Report. Organizations in general may choose to appoint a senior member of their Compliance, Internal Audit or Fraud Departments as MLRO. When several subsidiaries operate closely together within a group, there is much to be said for designating a single Money Laundering Reporting Officer at group level.

50. The Money Laundering Reporting Officer has significant responsibilities. He or she 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.

51. In making this judgment, he or she should consider all other relevant information available within the business concerning the person or client to whom 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, he or she decides that the initial report gives rise to knowledge or suspicion of money laundering and or the financing of terrorism, then he or she must disclose this information to the Financial Intelligence Unit.

52. The “determination” by the Money Laundering Reporting Officer implies a process with at least some formality attached to it, however minimal that formality might be. It does not necessarily imply that, the MLRO must give
his or her reasons for negating, and therefore not reporting any particular matter, but it clearly would be prudent, for the MLRO’s own protection, for internal procedures to require that only written reports are submitted to the MLRO and that the MLRO should record his or her determination in writing, and the underlying reasons therefore. Such documentation may be essential to substantiate any decision made by the MLRO should the need arise at the level of Board of Directors or in Court proceedings.

53. The Money Laundering Reporting Officer will be expected to act honestly and reasonably and to make his or her determinations in good faith when making a decision to file a Suspicious Transaction Report (STR).

Procedures for Reporting Suspicions to the MLRO

The need for simple reporting lines

54. Reporting lines for suspicions should be as short as possible, with the minimum number of people between the person with the suspicion and the MLRO. The hallmarks of an effective internal reporting system are speed, confidentiality, easy accessibility to the MLRO and the maintenance of full and accurate records.

55. The reporting requirements and procedures should be communicated to all employees. This can be done in a comprehensive but user-friendly handbook for management and staff. It is essential that employees are kept informed of changes to the reporting procedures. This includes the identities of those designated to receive the reports. If staff have been trained adequately and kept informed of the structure of their organization, they will know how, when and to whom their suspicions should be reported.

56. All procedures should be documented in appropriate manuals. Job descriptions should clearly state the accountabilities and responsibilities of those who are designated to handle suspicious activity reports.

57. The accountability for all reports, both those passed to FIU and those that are set aside, rests with the MLRO. The MLRO is required to sign off on all reports sent to FIU and regularly review those cases where:
   - the Money Laundering Reporting Officer has not yet made a decision on whether or not to file an STR;
   - no decision has been rendered by the FIU or law enforcement; and
   - the facility is being monitored internally by the financial institution.

The Role of Managers and Supervisors in the Reporting Process

58. The requirement to report suspicions can be a daunting prospect to a junior member of staff. In smaller organizations it may be possible for the person with the suspicion to discuss it with the MLRO and for the report to be prepared jointly. Alternatively, larger organizations may require the person
with the initial suspicion to refer it initially to a manager or supervisor to assess whether there are known facts that will remove the suspicion.

59. However, all MLROs must be aware that, they may not be deemed to have a reasonable excuse for failing to report promptly, if an ineffective reporting chain delays an internal report that could have assisted an investigation.

60. Once the reporting process has begun, and in order to comply with the Regulations, the report must reach the MLRO. In cases where the suspicion has been referred to a manager or supervisor, he or she should add to the report the information that is believed to remove the suspicion before passing it on to the MLRO.

61. Initial enquiries between colleagues to enable a member of staff to understand the nature and background of the transaction will not necessarily give rise to the need for an STR. However, if the employee is not satisfied with the clarification he/she receives, a report must be made. All employees must be advised that, the decision whether or not to report a suspicion to the MLRO remains with the employee and cannot be “delegated upward” to a manager or supervisor.

62. The MLRO should take into account any views and information provided by managers or supervisors, but must not permit them to “second guess” the member of staff. This particularly applies, if the manager or supervisor is earning a commission or bonuses from his/her subordinate’s activities.

**Internal Report Documentation**

63. All suspicions reported to the MLRO must be documented. Internal suspicious reports should include:
- the reporting department or branch;
- full details of the customer/client, including name, address, date of birth, occupation or profession and nationality or country of residence;
- as full a statement as possible of the information, which has given rise to the suspicion;
- the date on which the person with the suspicion first received the information and became suspicious;
- any connected accounts of which, the person who is reporting is aware;
- whether consent to complete the transaction/activity is required; and
- the date and time of the report.

64. Some institutions require the person with the suspicion and his/her manager to sign the report. Other institutions feel that anonymity of the staff is best maintained by not allowing them to sign internal reports of suspicion. It is for the institution to decide which procedures to adopt.
Acknowledgement of an Internal Report

65. The MLRO should acknowledge receipt of the suspicious activity report in writing to the reporting department or branch or direct to the reporting employee.

66. The MLRO should take this opportunity to remind the staff concerned of their obligation to do nothing that might prejudice enquiries, i.e. “tipping-off”. This offence could be committed through contact with the customer or the disclosure of information to a third party, regardless of whether it is known that the disclosure has been passed on to the FIU.

67. If there are any tapes or recordings of discussions with the customer or client, or any relevant evidence from surveillance equipment, the MLRO should ensure that they are retained.

68. The MLRO should remind relevant management and staff that the submission of a suspicious report in respect of an account or customer does not remove the requirement to submit further reports. If suspicions continue to arise in respect of other transactions or activity for the same customer, these should be reported internally.

MLRO Evaluation Process

69. The financial institution’s MLRO must consider each internal suspicious report and determine whether it gives rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion.

70. If the MLRO believes that a Suspicious Transaction Report requires no further examination, he/she must make a report to the FIU immediately, explaining that no further internal enquiry was considered necessary.

The MLRO’s Decision

71. All internal suspicions must be considered and documented without delay. Time may be of the essence, especially if the transaction has not yet taken place or is incomplete. In such circumstances, the financial institution may seek guidance from the FIU on the matter, but the ultimate decision to complete or not to complete the transaction will rest with the financial institution itself.

72. After making internal enquiries, the MLRO must decide whether or not the suspicious report is well founded, based upon reasonable grounds to suspect that the funds or activity are linked to criminal conduct or terrorist activity. If this is so, then the MLRO must submit the disclosure to the FIU to avoid committing the offence of failing to report. The enquiries undertaken, the decision and the reasoning behind the decision should be documented and retained securely. This information will be required either for the disclosure itself, or as evidence of good practice and best endeavor, if at some future date there is an investigation and the suspicions are confirmed.
No MLRO is expected to be infallible in validating reports of suspicions, or deciding whether or not to make a disclosure. Decisions which, with hindsight, prove to have been wrong, will not constitute prime facie evidence of non compliance (or of money laundering or terrorism financing), providing that the reasons for non-disclosure are justified, fully documented and retained with the original suspicious report.

Once the decision has been made to make a disclosure to the FIU, the MLRO should inform the reporting member of staff and the supervisor or line manager as appropriate and remind them that any further suspicious activity should be reported to the MLRO without delay.

IX - WHAT IS A SUSPICIOUS TRANSACTION?

“Suspicion” is personal and subjective and falls far short of proof based on hard evidence. However, it is more than mere speculation and is based on some foundation. Suspicious Transactions are financial transactions in which there are reasonable grounds to suspect that, the funds involved are related to the proceeds of criminal activity. What is reasonable depends on your particular circumstances, industry, normal business practices within your industry.

A suspicious transaction will often be one, which is inconsistent with a customer’s known legitimate business, activities or lifestyle or with the normal business for that type of financial services product. It follows that an important pre-condition of recognition of a suspicious transaction is for the financial services business to know enough about the customer’s business to recognize that a transaction, or a series of transactions, is unusual. However, should potential business be declined on the basis of a suspicion or belief that the assets which the potential customer wants to place are derived from or used in connection with criminal conduct, then this should also be reported to the FIU.

Although these Guidelines tend to focus on new business relationships and transactions, financial services business should be alert to the implications of the financial flows and transaction patterns of existing customers, particularly where there is significant, unexpected and unexplained change in the behavior of a customer in his use of a financial services product. Long-standing clients should not be overlooked in respect to identifying suspicious transactions.

Against such patterns of legitimate business, suspicious transactions should be recognizable as falling into one or more of the following categories:

- transactions which have no apparent legitimate purpose and/or appear not to have a commercial rationale;
• transactions, instructions or activity that involve apparently unnecessary complexity;
• where the transaction being requested by the customer, without reasonable explanation, is out of the ordinary range of services normally requested, or is outside the experience of a financial services business in relation to the particular customer;
• where, without reasonable explanation, the size or pattern of transaction is out of line with any pattern that has previously emerged;
• where the customer refuses to provide the information requested without reasonable explanation;
• where a customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period of time;
• the extensive use of trust or offshore structures in circumstances where the customer’s needs are inconsistent with the use of such services;
• transfers to and from high risk jurisdictions, without reasonable explanations, which are not consistent with the customer’s declared business dealings or interests;
• unnecessary routing of funds through third party accounts;
• unusual investment activity with no discernable purpose.

This however is not an exhaustive list.

79. The following factors should be borne in mind when seeking to identify a suspicious transaction of instruction:

(a) Is the customer known personally?
(b) Does the transaction or activity make sense for that particular customer?
(c) Is the transaction in keeping with the normal practice in the market to which it relates i.e. with reference to market, size and frequency?
(d) Is the role of any agent involved in the arrangement unusual?
(e) Is the transaction to be settled in the normal manner?
(f) Are there any other transactions or activity linked to the transaction in question which could be designed to disguise the money and divert it into other forms or other destinations or beneficiaries?
(g) Are the reasons for the transaction transparent and understandable, i.e. is there a cheaper, easier or more convenient method available?

80. The Money Laundering Reporting Officer (MLRO) should be well versed in the different types of financial products and services, which his business provides to its clientele and which may give rise to opportunities for money laundering and financing of terrorism.

81. Further, International standards for detection and prevention of money laundering now recognize that money laundering is a risk that needs to be managed taking a proportionate approach. With out a risk-based approach,
cost would be disproportionate, the effectiveness of the system would be
diluted and the requirements would be over burdensome for financial
institutions and other relevant businesses.

82. The risk-based approach places the responsibility on senior management to
identify and assess the money laundering risks and to take measures to
manage and monitor those risks within the framework of these Guidelines.
Money laundering and Customer Due Diligence/Know Your Customer risks
are closely linked to risks that arise in other areas of a financial institution’s
business, and these risks need to be managed as a whole.

X – REPORTING OF SUSPICION

ALL SUSPICIOUS TRANSACTIONS

83. Businesses and institutions in The Bahamas have a statutory obligation to
put in place procedures, systems and controls to ensure that their employees
recognize and report circumstances: (a) where they know; or (b) where they
suspect; or (c) where there are reasonable grounds to know or suspect that
their products, services or facilities are being used for the purposes of
money laundering or terrorism financing.

84. The key to recognition of knowledge, suspicion or where there are
reasonable grounds for knowledge or suspicion, is knowing enough about
the client and his business. This leads one to recognize that a transaction, or
series of transactions, or a particular instruction is unusual or unexpected or
does not represent legitimate activity.

85. Reporting of a suspicion of criminal conduct is important as a defense
against a possible accusation under the relevant Bahamian laws of assisting
in the retention or control of the proceeds of crime. In some circumstances,
a failure to report can be an offence. In practice, a Money Laundering
Reporting Officer will normally only be aware of having a suspicion of
criminal conduct, without having any particular reason to suppose that the
suspicious transactions or other circumstances relate to the proceeds of one
sort of crime or another.

86. Financial services business should ensure that:
   • all staff know to whom their suspicions of criminal conduct should be
     reported;
   • there is a clear procedure for reporting such suspicions without delay to
     the Money Laundering Reporting Officer;
   • the MLRO should have sufficient level of authority and independence
     within a financial institution to enable him/her to carry out his function.

87. Staff should be required to report any suspicion of laundering of the
proceeds of crime directly to their Money Laundering Reporting Officer.
Financial services businesses are not expected to perform the role of
detectives but rather, the MLRO will be expected to gather the relevant facts and make a decision to report or not report to the FIU.

88. For almost all suspicious transaction reports, financial services business can detect a suspicious or unusual transaction involving criminal conduct but cannot determine the underlying offence. They should not try to do so. There is a simple rule, which is that, if a suspicion of criminal conduct is aroused, then report the same to the FIU.

89. Employees will meet their obligations, in this regard, if they comply at all times with the policy and procedures of their financial services business, and will be treated as having performed their duty to report under the relevant laws, if they disclose their suspicions regarding proceeds of criminal conduct to their Money Laundering Reporting Officer, according to such corporate policies/procedures, as may be in operation in their financial services business. This confirmation is enshrined within Regulation 5 of the Financial Intelligence (Transactions Reporting) Regulations, 2000 and the Proceeds of Crime Act, 2000. An employee, employed at the relevant time, and who makes a disclosure in accordance with his or her employer’s disclosure procedures, has a defence in the event of any proceedings.

90. On receipt of a report concerning a suspicious customer or suspicious transaction, the Money Laundering Reporting Officer should determine whether the information contained in such report supports the suspicion. He should investigate the details in order to determine whether, in all the circumstances of the particular case, he should promptly submit a report to the FIU.

91. If the Money Laundering Reporting Officer decides that the information does substantiate a suspicion of money laundering or terrorism financing, he should disclose this information promptly to the FIU. If he is genuinely uncertain as to whether such information substantiates a suspicion of criminal conduct, he should still report to the FIU. If, in good faith, he decides that the information does not substantiate a suspicion, and he does not report any suspicion, there will be no liability for non-reporting, if the judgment is later found to be wrong, but the reasoning and judgment that is relied upon not to report should be documented and retained.

92. Local financial legislation imposes a duty on financial institutions to maintain confidentiality in regard to the affairs of their customers. However, there are exceptions for breach of this duty enshrined in Bahamian legislation and common law.

93. Where Suspicious Transaction Reports are filed, pursuant to the relevant Bahamian legislation, a licensee may in addition thereto, make a determination to also, subject to its group/corporate Policies and Procedures, corporate relationships, etc., inform the Compliance
Department/Committee at Head Office of its suspicions within the financial services business/group. It is important to note however, that any report made by a financial institution to its Head Office/group outside The Bahamas should not, under any circumstances, be seen as removing the need to comply with local legislation, which also imposes an obligation to maintain client/customer confidentiality as well as to file an STR with the Financial Intelligence Unit.

94. Financial services businesses with a regular flow of potentially suspicious transactions are strongly encouraged to develop their own contacts with the FIU and periodically to seek general advice from the FIU as to the nature of transactions, which should or should not be reported.

RECOGNITION OF SUSPICIOUS TRANSACTIONS

95. As the types of transactions, which may be used for criminal purposes, are almost unlimited, it is difficult to define a suspicious transaction. However, a suspicious transaction will often be one, as aforesaid, which is inconsistent with a customer’s known, legitimate business or personal activities or with the normal business for that type of account. Therefore, the first key to recognition is knowing enough about the customer’s business to recognize that a transaction, or series of transactions, is unusual. Efforts to recognize suspicious circumstances should commence with the request to open an account or execute the initial transaction.

EXAMPLES OF SUSPICIOUS TRANSACTIONS

96. Examples of what might constitute suspicious transactions are given in Appendix G. These are not intended to be exhaustive and only provide examples of the most basic ways by which money may be laundered.

REPORTING OF SUSPICIOUS TRANSACTIONS

97. There is a statutory obligation on all employees to report suspicions of money laundering and or terrorism financing to the Money Laundering Reporting Officer (MLRO) in accordance with regulation 5 of the Financial Intelligence (Transactions Reporting) Regulations, 2000. For this purpose, detailed Policies and Procedures must be readily available to all employees. Once an employee has reported his or her suspicion to the MLRO, he or she has fully satisfied the statutory obligation.

98. Where a financial institution chooses to out source a function within its organization/group (e.g. account opening, formation of legal persons/arrangements, transactions processing, account administration, etc,) or to another party situated locally or in another jurisdiction, and the agent, operating under this arrangement, formulates a suspicion about a particular transaction, the agent must immediately submit an internal report on the matter to the Money Laundering Reporting Officer for the financial
institution. The MLRO will review such a report and make a determination as to whether or not to file a Suspicious Transaction Report with the FIU.

**XI – MONITORING METHODS AND PROCEDURES**

99. When considering how best to monitor customer transactions and behavior, financial institution should take into account:

(a) the size and complexity of its business;
(b) its business risk assessment;
(c) the nature of its systems and controls;
(d) the monitoring procedures that already exist to satisfy other business needs; and
(e) the nature of the products and services and the means of delivery.

Methods to be considered include:

(a) simple exceptions reports to advise supervisors/operations managers of large transactions for their review;
(b) more complex exceptions reports to advise the MLRO, or other appropriate staff, of customers and transactions matching certain predetermined criteria;
(c) computerized transactions monitoring systems.

**MONITORING COMPLEX AND UNUSUAL TRANSACTIONS**

100. Financial institutions are reminded of the need to scrutinize transactions which are complex, large and unusual, or unusual patterns of transactions which have no apparent economic or lawful purpose.

101. Where such transactions are noted, financial institutions are obligated to undertake procedures to examine the purpose and background of the transactions or circumstances. This may involve making enquiries of the customer and asking questions an honest man would reasonably ask himself in the circumstance. Such enquiries, when conducted properly and in good faith do not constitute tipping off where:

(a) a suspicious transaction report has not yet been made to the FIU;
(b) the financial institution itself has no reason to believe a suspicious transaction report has been made to the FIU;
(c) the financial institution has no knowledge of or reason to believe that an investigation of the customer is about to be started or already underway by the relevant authorities.

102. In addition, if CDD information and documentation was not obtained at the time the relationship was commenced or it is inadequate, financial
institutions must take steps to obtain the relevant documentation and information.

103. These enquiries can be addressed using a customer service approach. They are directly linked to the CDD requirement, and indicate the importance of knowing your customer in detecting unusual or suspicious activity. Where there is any suspicion, a report must be made to the FIU using the disclosure form found in Appendix H.

**CONSIDERING UNREASONABLE CUSTOMER INSTRUCTIONS**

104. A customer who is, or may be, attempting to launder money will frequently structure his instructions in such a way that the economic or lawful purpose of the instruction is not apparent or is absent entirely when asked to explain the circumstances or transactions, the customer may be evasive or may give explanations which do not stand up to reasonable scrutiny.

105. Where the financial institution is suspicious, or has knowledge of, money laundering or terrorist financing, it should not unquestioningly carry out instructions exactly as issued by the client.

106. If a financial institution unquestioningly carries out unreasonable instructions in this manner, it may mean that it is failing in its duty to forestall and prevent money laundering and terrorist financing, and in extreme circumstances may place itself in a position of potentially being construed to have assisted money laundering or terrorist financing.

**HANDLING CASH TRANSACTIONS**

107. Where cash transactions are being proposed by customers, and such requests are not in accordance with the customer’s known reasonable practice, financial institutions must approach such situations with caution and make relevant enquiries.

108. Where the financial institution has been unable to satisfy itself that any cash transaction is reasonable activity, and therefore considers it suspicious, a suspicious transaction report should be made to the FIU.

**“HOLD MAIL” RELATIONSHIPS**

109. "Hold Mail" accounts are accounts where the account holder has instructed the Licensee not to issue any correspondence to the account holder's address.

110. Regardless of the source of "Hold Mail" business, evidence of identity of the account holder should be obtained by the financial institution in
accordance with Section VI of these Guidelines.

111. It is recommended that Licensees 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 Licensee’s file.

112. 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 Licensees should monitor such accounts more closely as these accounts may represent additional risk.

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

XII - REPORTING TO THE FINANCIAL INTELLIGENCE UNIT (FIU)

114. Pursuant to Section 14 of the Financial Transaction Reporting Act, 2000, as amended, all financial institutions are ‘obligated’ to report Suspicious Transactions to the Financial Intelligence Unit.

115. Further, all financial institutions are required to establish a point of contact with the Financial Intelligence Unit in order to handle the reported suspicions of their staff regarding money laundering and or the financing of terrorism. Such institutions are required to appoint a “Money Laundering Reporting Officer” to undertake this role, and this officer has to be registered with the Financial Intelligence Unit. Financial institutions are also required to appoint a “Compliance Officer” who shall ensure full compliance with the laws of The Bahamas (see Regulation 5 of the Financial Intelligence (Transactions Reporting) Regulations, 2001). Alternatively, one officer can hold both positions simultaneously.

116. Where an entity does not provide the financial services outlined in Section V of these Guidelines, such an entity is not a financial institution and is therefore not required to register a Money Laundering Reporting Officer (MLRO) with the Financial Intelligence Unit. It is advisable that the entity consults with its respective relevant regulatory agency regarding the identification and appointment of a MLRO and or Compliance Officer.

117. If the Money Laundering Reporting Officer decides that a disclosure should be made, a report, preferably in standard form (see Appendix H), should be sent to the FIU. Financial services businesses should also append to the standard form any copies of additional information (e.g. statements, internet
searches, contract notes, correspondence, minutes, transcripts, etc.) that will assist the FIU in understanding the basis upon which the suspicion was raised. The financial services business should provide full evidence to support the grounds upon which the Suspicious Transaction Report has been filed with the FIU.

118. If the Money Laundering Reporting Officer considers that a report should be made urgently (e.g. where the customer’s financial services product is already a part of a current investigation), initial notification to the FIU should be made by telephone and the same should be followed up in writing as soon as practicable. The receipt of a report will be promptly acknowledged in writing by the FIU with a letter similar to that in Appendix J. To the extent permitted by law, financial services businesses should comply with any instructions issued by the FIU. In all cases, the FIU will acknowledge receipt of the financial institution’s report. The report is forwarded for review to a trained FIU Analyst who, alone, has access to it. The Analyst may seek assistance or further information from the reporting financial services business and, in addition, may use other sources for conducting his assessment of the report.

119. Discreet inquiries are made by the Analyst to confirm the basis for a suspicion but the customer is never approached. In the event of a prosecution, the source of the information is protected. Production Orders are used to produce such material for the Court. Maintaining the integrity of the confidential relationship between law enforcement agencies and financial services businesses is of paramount importance to the FIU.

120. Financial institutions should consider maintaining a register of all suspicious reports made to the FIU. Such register should contain the following details:

- the date of the report;
- the person who made the report;
- the person(s) to whom the report was forwarded;
- a reference by which supporting evidence is identifiable; and
- status reports on the account, any further transactions and or actions taken by the FIU and the financial institution.

**FEEDBACK FROM THE FIU**

121. The provision of feedback to financial services businesses is one of the key roles of the FIU. It is vital that intelligence/trends relating to new money laundering methods, financing of terrorism and other financial crime are imparted to the financial sector to enable it to prevent the services offered from being abused/utilized by criminals.

122. In practice, the FIU delivers feedback in a number of different ways:
• taking an active role and participating in key local financial crime seminars, directly by speaking to the various associations and through other training organized by the FIU; and
• where ever possible, dealing directly with the financial services businesses that makes suspicious transaction reports.

TIPPING OFF
123. The relevant laws include “tipping off” offences. However, it is a defence to prove that the person did not know or suspect that the disclosure was likely to be prejudicial in the way mentioned in that subsection. Therefore, preliminary enquiries of a customer or client by key staff (or any other staff of a financial services business) either to obtain information or confirm the true identity, or ascertain the source of funds or the precise nature of the transaction to be undertaken, will not trigger off the offence before a suspicious transaction report has been submitted in respect of that subject, unless, the enquirer has prior knowledge or suspicion of a current or impending investigation.

124. For an offence to be committed, tipping off a suspect must be undertaken knowing or suspecting the consequences of the disclosure. Enquiries to check whether an unusual transaction has genuine commercial purpose will not be regarded as tipping off.

125. There will be occasions where it is feasible for the financial services business to agree a joint strategy with the FIU to ensure that the interests of both parties are taken into account.

RETENTION OF RECORDS
126. The Proceeds of Crime Act provides, inter alia, for the Court to determine whether a person has benefited from crime, and to assume that certain property received by that person conferred such a benefit. Accordingly, the investigation involves reviewing the audit trail of suspected criminal proceeds by, for example, supervisors, auditors and law enforcement agencies and establishing a financial profile of the suspected financial services product. Therefore, it is important to retain records for the statutory period, in order to assist in the aforementioned process.

TIME LIMITS
127. In order to facilitate the investigation of any audit trail concerning the transactions of their customers, financial services businesses should observe the following:

• financial services businesses shall retain each customer’s verification documentation in its original form for at least the minimum statutory retention period, which is currently five years; and

• financial services businesses shall retain each customer document (that is not a customer verification document) in its original form, or a complete copy of the original, certified by a manager, partner or director
of the financial services businesses, for at least the minimum statutory retention period.

128. Where the FIU is analyzing a suspicious transaction report, it may request a financial services business to keep records until further notice, notwithstanding that the prescribed period for retention has elapsed. Even in the absence of such a request, where a financial services business knows that an investigation is proceeding in respect of its customer, it should not, without the prior written approval of the FIU, destroy any relevant records, even though the prescribed period for retention may have elapsed.

**XIII - REPORTING PROCEDURES**

129. 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.

130. The use of a standard format in the reporting of disclosures is important and should be followed. The form illustrated in Appendix H should be used and the information must be typed. Disclosures can be forwarded to the Financial Intelligence Unit in writing, by post, by facsimile message, or by electronic mail. In cases of urgency, reports may be made orally.

131. Sufficient information should be disclosed in order to provide the nature of and reason for the suspicion. Where the financial institution has additional relevant evidence that could be made available, the existence of this evidence should also be clearly indicated.

132. The Financial Intelligence Unit will acknowledge the receipt of a disclosure formally. Normally, completion of a transaction or operation of the customer’s account will not be interrupted. However, in exceptional circumstances, such as the imminent arrest of a customer and consequential restraint of assets, the bank will be required to discontinue the transaction or cease operation of the customer’s account, based upon actions taken by the FIU’s issuance of a Freeze Order, pursuant to Section 4(2)(b) of the Financial Intelligence Unit Act.

133. Access to the disclosure is restricted to Financial Analysts and other officers within the Financial Intelligence Unit. Maintaining the integrity of the confidential relationship, which has been established between the Financial Intelligence Unit, law enforcement agencies and financial institutions, is considered to be of paramount importance and will be maintained for the integrity of the information received.

134. It is recognized that the provision of information inviting the inference that a customer is suspected of involvement in criminal conduct might have an
influence on the commercial decisions made subsequently by the disclosing institution.

135. It is also recognized that as a result of a disclosure, a financial institution may leave itself open to risks as a **constructive trustee** if moneys are paid away other than to the true owner. The financial institution must therefore make a commercial decision as to whether funds, which are the subject of any suspicious transaction report (made either internally or to the Financial Intelligence Unit), should be paid away under instruction from the account holder.

136. Financial institutions are reminded that reporting to entities identified in **Section 18 of the Financial Transactions Reporting Act, 2000, as amended**, will provide similar protection against breach of confidentiality. It is therefore recommended that to reduce the risk of constructive trusteeship when fraudulent activity is suspected, and to obtain the fastest possible Financial Intelligence Unit response, disclosure should be notified by telephone and a completed disclosure form forwarded to the Financial Intelligence Unit. Where timing is believed to be critical, a financial institution should prepare a back-up package of evidence for rapid release on the granting of a court order, search warrant, or a freezing order pursuant to section 4(2)(c) of the Financial Intelligence Unit Act, 2000.

137. The FIU recognizes the need for balance by a financial institution between promoting an on-going commercial relationship with its clientele and simultaneously maintaining dialogue with the FIU itself. However, should it become necessary after an STR has been filed to terminate a facility, it would be helpful if the financial institution would notify the FIU of this decision and to provide details as to the proposed change in the status of the facility. Similarly, where the client initiates closure of the facility, the FIU would appreciate being informed in advance of such closure.

**XIV - MONEY TRANSMISSION BUSINESSES**

138. Money Transmission Business ("MTB") is as defined in **Section 2 of the Banks and Trust Companies Regulation Act, 2000**, 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.

139. A “money transmission service provider” is defined as any person carrying on a money transmission business.

140. A “money transmission agent” is defined as any person carrying on money
transmission business on behalf of a money transmission service provider.

141. In accordance with Section 3(1)(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 there under.

142. It is the responsibility of each MTB to have policies in place 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 in recognising and reporting suspicious transactions.

Vulnerability of MTBs to Money Laundering & Terrorist Financing

143. 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.

144. 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 XV of these Guidelines) that should accompany wire transfers to mitigate the abovementioned risk.

145. 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

146. 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 XV on "Electronic Payments Transfers" set out below.

147. 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.

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

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

Transaction Monitoring

150. 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

151. 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 Licensee'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 at different times on the same day; with different MTB cashiers on the same day or different days; and at different branches/offices of the same MTB.
- Transactions that cannot be reconciled with the usual activities of the customer.
- A 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 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.

**XV - ELECTRONIC PAYMENTS TRANSFERS**

152. **The Financial Action Task Force (FATF)** in its revised Recommendations dated February 2012, issued **Recommendation 16 (formerly Special**
Recommendation VII or SR VII) with the objective of enhancing the transparency of cross-border and domestic electronic payment transfers (“wire transfers” or “transfers”) thereby making it easier for law enforcement to trace funds transferred electronically by terrorists and other criminals. SR VII has been implemented in The Bahamas through the Financial Transactions Reporting (Wire Transfers) Regulations, 2009 (“the Wire Transfers Regulations”).

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. Generally, the Wire Transfers Regulations require financial institutions that participate in the execution of wire transfers to obtain and retain specified information on payers of wire transfers and to ensure that all transfers through the payment chain are accompanied by information on the payers who give the instructions for payment to be made.

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

Licensees that initiate wire transfers on behalf of payers (“originating financial institutions”) must ensure that the payer information conveyed in the payment message or instruction is accurate and has been verified.

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, 2000 and the FTRR, 2000 as amended. In such cases, the originating financial institution may assign to the wire transfer a unique identifier that would link the account holding customer and his relevant identification information to the wire transfer.

Before initiating one-off wire transfers on the instructions of non-account holding customers, originating financial institutions must verify the identity and address (or a permitted alternative to address) of the payer.

Originating financial institutions may apply simplified due diligence for wire transfers below $1,000 provided that such transfers are considered to present a low risk of money laundering or terrorist financing.

Cross-border Wire Transfers - Complete Payer Information

Except as permitted below, complete payer 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 consists of the payer’s:

(a) name;
(b) account number, or if no account exists, a unique identifier or transaction number; and
(c) address, or date and place of birth, or national identity number, or customer identification number.

159. 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, 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.

160. Where the wire transfer is not debited to a bank account, the requirement for an account number must be substituted by a unique identifier or transaction number which permits the transfer to be traced back to the payer. The Wire Transfers Regulations define “unique 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 affect the transfer of funds”. Similarly the “Transaction number” should identify and link a particular payer to the wire transfer.

161. 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 may be used for payers resident in countries that issue such numbers. However, for payers resident in other countries, it must be remembered that other numbers such as a National Insurance or Social Security number, passport number or driver’s license number are not National Identity Numbers. 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, or may be a number contained in an official document such as National Insurance or Social Security number, passport number or driver’s license number.

162. 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.

163. 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**

164. 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 identifier or a transaction number which permits the transaction to be traced back to the payer. 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**

165. A batch file transfer contains several individual transfers from a single payer bundled together for transmission to beneficiaries outside The Bahamas. For batch file transfers of $1,000 or more, a hybrid complete/reduced payer information requirement applies. Individual transfers within the batch file need carry only the payer’s account number or a unique identifier or transaction number, provided that the batch file itself contains complete payer information.

**Wire Transfers via Intermediaries**

166. Intermediary financial institutions are Licensees, other than originating or beneficiary financial institutions that participate in the execution of funds transfers. Intermediary financial institutions must, subject to the following guidance on technical limitations, ensure that all information received on the payer which accompanies a wire transfer is retained with the transfer throughout the payment chain.

**Technical Limitations**

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

(a) if it is aware that the payer information is missing or incomplete it must concurrently advise the beneficiary 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 information received with the funds 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, the intermediary financial institution must provide the payer information received with the funds transfer within three business days of receiving the request.

Minimum standards

168. The above information requirements are minimum standards. It is open to Licensees 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

169. 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 (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 Payments

170. The Wire Transfers Regulations specify that beneficiary financial institutions should adopt risk based procedures to detect whether required 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.

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

(a) SWIFT payments on which mandatory payer 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 non-compliant 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 Licensees‘ 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.

172. 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.

173. Where an originating financial institution is identified as having regularly failed to comply with the payer 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.

174. 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**

175. 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**

176. As indicated in paragraph 175 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 Primary Account Number (PAN) serves this function.

177. 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**

178. 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 not exceeding $2,000.
179. The term “cash courier” refers to an individual who physically transports, mails, ships, or causes to be physically transported mailed, shipped currency or monetary instruments. This term is not intended to include persons engaged in money remittances as licenced businesses.

180. Cash smuggling is one of the major methods used by terrorist financiers, money launderers and organized criminals to move money derived through illegal means to support their activities. In cash smuggling operations, couriers will, inter alia, travel by road, through airports or by lake or sea with loads of cash, often stuffed in boxes, suit cases and concealed compartments in vehicles and on persons.

181. The Financial Action Task Force (FATF), in its revised Recommendations dated February 2012, issued Recommendation 32 (formerly Special Recommendation IX or SR IX) with the objective of preventing the physical cross border transportation of currency and bearer negotiable instruments via the use of a declaration system and/or a disclosure system. Under this provision, the competent authorities must have the legal authority to stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing, money laundering or predicate offences or that are falsely declared or disclosed. The Bahamas is in the process of putting in place the requisite institutional arrangements to comply fully with Recommendation 32.

RESPONSE TO COORDINATED GLOBAL ACTION

182. More stringent laws against money laundering, along with anti-money laundering measures adopted globally by traditional financial institutions, have forced criminal organizations to shift the movement of their illicit proceeds outside of the established financial industry. To avoid the scrutiny of law enforcement, these criminal organizations increasingly have resorted to non-traditional methods to move funds, including the smuggling of bulk cash across borders.

183. Bulk Cash Smuggling (BCS) is a result of criminal activity, with sources of illicit income including human and contraband smuggling, bribery, extortion, fraud, and illegal gambling. BCS occurs as the money from criminal activities travel from location to location for collection by higher levels of management in a criminal organization. Criminal enterprises, just like other businesses, can’t operate without a steady cash stream. Suspicious transaction reports (STRs) assist investigators with flagging potential criminal activity, identifying criminally derived assets and disrupting criminal financial flows.
**XVII - USE OF THE FINANCIAL SYSTEM**

184. Terrorists, and those financing terrorists, have used the following financial services products to transfer and launder their funds:

(i) bank accounts (including the targeting of previously dormant accounts which are re-activated);

(ii) electronic transfers (wire transfers); and

(iii) money services business.

The case studies in Appendix B provide examples of the trends outlined above.

**XVIII - SOURCES AND USES OF FUNDS**

**FUNDING SOURCES**

185. As indicated in the diagram immediately below/overleaf, terrorist financing may be derived from legitimate or illegitimate sources. It may be derived from criminal conduct, i.e. counterfeiting, 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 organizations.

**USES OF FUNDS**

186. Terrorists require funds to support their activities and must move those funds to individuals or cells in particular target areas. The amounts needed for a particular activity or purpose may be relatively small, but larger amounts are needed to recruit, transport, train, house, pay and equip their agents and to support family members of related parties. Terrorist financiers may use known money laundering methods, informal value transfer systems known and even traditional financial institutions and mechanism to hide the sources, purpose and movement of their assets.
FIU’S GUIDELINES
FOR FINANCIAL INSTITUTIONS - 2013

Terrorist Funding

- Burglary
- Theft
- Robbery
- Drugs
- Fraud
- Counterfeit Currency
- Contributions
- Taxi
- Gaming
- Clubs
- Smuggling
- Extortion
- Counterfeit Goods
- Legitimate Business

Terrorist Financing

- Mainland
- Acts of Terrorism
- Prisoners' Families
- International
- On The Run
- Engineering
- Admin
- Training
- Weapons Procurement
- Volunteers
187. The relationship between business and client is essentially a contractual one and it provides the foundation for all economic activity. This relationship, on the one hand, is rooted in a need for a product or service on the part of the client, which invariably translates into an opportunity for an economic profit or gain on the part of the business, to the extent that the latter is able to satisfy the needs of the client. However, the relationship presents some risks to both parties. Money is the medium of exchange.

188. Understandably, the customer’s demands, coupled with competition in all of its forms among service providers/suppliers, weigh heavily on this relationship. Specifically, the client expects quality service at all times, with quality generally being defined in terms of reliability of service, minimum costs, minimum errors/defects, quick delivery and few inconveniences, etc.

189. In contrast, the business is challenged to justify its existence by generating a satisfactory profit on its operations. Survival, therefore necessitates both building a sustainable client base to ensure the business continues as a going concern. Evidence that this objective permeates most aspects of the business is seen in the way the business itself is structured departmentally.

190. The general scenario outlined in the three preceding paragraphs holds true for financial services as with other types of businesses.

XIX - RECORD KEEPING

191. Sections 23, 24 and 25 of the FTRA require financial institutions to retain for five years all 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.

192. 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 is to ensure, in so far as is practicable, that in any subsequent investigation a financial institution can provide the authorities with its section of the audit trail.

193. In addition to retention of customer identification and transactions records financial institutions are also required to maintain records of suspicions which were raised internally with the MLRO but not disclosed to the authorities. Records of suspicions which the authorities have advised are of no interest should be retained for a similar period. Likewise, records of a Licensee’s
findings of their enquiries into unusual activities, should also be retained for a minimum of five years.

194. Financial institutions are also required to keep records of on-going staff training with respect to prevention of money laundering and financing of terrorism.

195. It is recognized that, financial institutions will find it necessary to rationalize 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).

196. Financial institutions 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.

XX – SIGNIFICANT TRENDS WITH IMPLICATIONS FOR FINANCIAL SERVICES

197. Since the last revision of these Guidelines in 2007, a number of trends, as detailed below, have emerged locally, while others have become more pronounced and challenging from a supervisory/law enforcement perspective necessitating legislation by Parliament. Individually and collectively, these developments have implications for financial institutions, particularly with respect to internal procedures (i.e. KYC/CDD, record keeping, staff training, suspicious transactions reporting) mandated by law to prevent money laundering and terrorism financing. In view of the threat presented in each instance, financial institutions are reminded of the need for vigilance as criminal elements continue to resort to creative methods to get criminally derived proceeds into the financial system in order to ultimately benefit from the proceeds of these criminal acts.

CASH FOR GOLD

198. As with copper and other metals, the demand for gold on global commodity markets has contributed to a record increase in its price. Locally, this has translated into an increase in incidents of theft, house breakings, robberies and in some cases murder, with the perpetrators, immediately after such incidents, trying to sell the stolen items for ‘cash’ to cash for gold dealers. In 2011, Parliament approved the Pawnbrokers and Secondhand Dealers Act, 2011, in an effort to deal with this problem. Law enforcement agencies have reported significant recoveries of apparent stolen items confiscated from raids carried out on cash for gold establishments in accordance with
the provisions of the Act.

**COPPER AND SCRAP METAL**

199. The demand for copper and certain other metals on global commodity markets have contributed to an increase in the price of such items. Locally, this has resulted in an increase in theft of copper and other scrap metals from private residences, businesses, governmental agencies, churches, cemeteries, construction sites, etc. The subsequent sale of stolen items to scrap metal dealers for ‘cash’ payments and eventual export of the items by the dealers for substantial profits prompted the approval by Parliament of the [Pawnbrokers and Secondhand Dealers Act, 2011](#).

200. The primary purpose of the Act is to monitor the activities of pawn brokers, deter unlawful property transactions through pawn brokers and secondhand dealers and to facilitate the efforts of law enforcement in stolen goods. The passage of the Act was preceded in July 2011 by an order by the government which placed a ninety (90) day ban on scrap metal exports and a permanent ban on copper exports. The export of scrap metals and copper has since resumed with export of the latter being allowed on a strictly controlled basis. Notwithstanding this, copper theft continues to be a major challenge for law enforcement.

201. Offences under the Act, include the following, namely, any person who:-

(a) fails to obtain a licence in accordance with the Business Licence Act;
(b) knowingly furnishes false information under this Act or any regulation made there under;
(c) fails to keep any books or records required to be kept;
(d) fails to furnish any returns required to be furnished;
(e) knowingly sells or pawns or attempts to sell or pawn off any stolen articles;
(f) fails to retain in unaltered state every article acquired during the course of his dealings for a minimum period of seven days from the date of the transaction;
(g) contravenes any provision of the Act.

202. Summary conviction under the Act attracts a fine not exceeding twenty thousand dollars or a term of imprisonment not exceeding two years, or both such fine and imprisonment.

**COUNTERFEIT PRODUCTS AND SMUGGLING**

203. In bound smuggling and sale of counterfeit products such as tobacco, cigars, cigarettes, beers, hand bags, etc, is contributing to a significant, annual revenue loss for Bahamas Customs Department. The Department estimates its annual loss on tobacco products alone to be in the region of $20Million.

204. Legitimate businesses negatively impacted by sale of counterfeit products have called on the central government for assistance in stopping such
activities as their survival is contingent upon effectively remediying this problem.

205. False invoicing, under invoicing and payment of bribes, reportedly, are just some of the methods used by perpetrators to circumvent paying correct rate of import duty on imported goods. These illegal activities constitute offences under the Customs Management Act and the Prevention of Bribery Act, Chapter 88 Statute Laws of the Bahamas and are subject, on conviction to a fine or prison sentence or both. Proceeds derived from such criminal activities are also subject to seizure and forfeiture under the applicable laws.

206. To remedy these and other on-going challenges face by the Department, a new Customs Management Act and Regulations were recently approved by Parliament and will be implemented in the near future.

CYBER CRIME

207. Cyber-crime is rapidly gaining attention, largely, because it is an entirely new form of crime. Most, though not all, cyber-crime is directly related to criminal activities that have existed in the bricks and mortar society for decades or longer. Indeed, these activities have taken on a scale and scope that was unknown just a few decades earlier and by all appearances, the criminal groups responsible for these crimes only gained the ability to expand their enterprises as a result of the American War on Drugs.

208. A generalized definition of cyber crime may be “unlawful acts wherein the computer is either a tool or target or both.” The computer may be used as a tool in the following kinds of activity: financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases: unauthorized access to computer/ computer system / computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

209. As detailed below, “cyber criminals” are broadly classified into four grouping depending upon their objectives.

- Children and adolescents between the ages of 6 – 18 years driven by a desire to know and explore things as well as to prove themselves among peers;

- Organized hackers who are motivated to penetrate corporate or public sites and databases in order to fulfil political objectives or fundamentalist ideology;
• Professional hackers / crackers who, motivated by money, are primarily employed to hack the sites of rivals to get credible, reliable and valuable information; in some case they are even employed to crack the system of their employer basically as a measure to make it safer by detecting loop holes early;

• Discontented employees who have either been terminated or are dissatisfied with their employer and as revenge, hack the system of their employer.

210. Cyber crimes may be directed against individuals in the form of harassing e-mails, cyber stalking, obscene material, indecent exposure, e-mail spoofing, defamation, cheating, fraud, viruses, bullying, computer vandalism, intellectual property, internet time theft or unauthorized access/control over computer system.

211. Cyber crimes directed against an organization may take the form of distribution of pirated software, cyber terrorism against a central government or agency, possession of unauthorized information i.e. trade secrets or unauthorized access/control over computer system.

212. Cyber crimes directed against society at large may take the form of pornography, indecent exposure, drug / human trafficking, financial crimes, sale of illegal articles, on-line gambling, terrorism and forgery.

213. Globalism and the internet have transformed radically the nature of criminal activity. In particular, the internet has made it easy for organized crime groups to commit crimes across borders, taking advantage of the obstacles which law enforcement officials encounter when trying to work together across international boundaries. This is particularly challenging for the global community, considering the linkage between narcotics trafficking and related criminal activities of money laundering, terrorism, human trafficking, and cyber-crime. This linkage can be traced in one way or another to the Drug War.

214. Closely related to cyber crime is the phenomenon of cyber laundering. This is a new way to hide the proceeds of crime. The advance of technological solutions of electronic payments and online gambling has eliminated the need for time and space as compared to the traditional way of money laundering to achieve Cyber laundering. Any means other than the provided ways to transfer goods and services using cyber space technologies and information systems for personal benefits using deception is considered as cyber laundering.

215. At present, no meaningful financial statistics are readily available to gauge the level of cyber crime at a global level, although anecdotal evidence would suggest same to be in the billions of dollars annually.
FATCA

216. Effective for payments after June 30, 2014, generally all foreign financial institutions (FFIs) will be required to enter into disclosure compliance agreements with the U.S. Treasury (unless an exemption or FATCA Intergovernmental Agreement applies), and all non-financial foreign entities (NFFEs) that are not excepted under the regulations must report and/or certify their ownership or be subject to the same 30 percent withholding.

217. This new reporting and withholding regime will ultimately impact current account opening processes, transaction processing systems and “know your customer” procedures utilized by foreign banks. Compliance Officers, tax reporting heads and other key players within financial institutions will need to evaluate the potential impact of these regulations and develop a plan for managing and remediating any potential risk associated with Foreign Account Tax Compliance Act (FATCA) non-compliance.

218. The Bahamas has opted to enter into a Model 1 Intergovernmental Agreement with the United States with regard to the implementation of FATCA.

FIREARMS TRAFFICKING

Illegal firearms trafficking is the movement of firearms from the legal to illegal marketplace through an illicit method for an unlawful purpose, usually to obtain profit, power, or prestige or to supply firearms to criminals or gangs.

219. Globally, smuggling has become the quintessential criminal activity of criminal organizations, and trafficking in firearms is, together with drugs and trafficking in persons, one of the most lucrative of such criminal activities. Available 2012 statistics estimates the market for illegal small firearms and light weapons at $1 Billion annually.

220. A comprehensive global treaty (The Arms Trade Treaty), designed to curb the movement of illegal firearms and ammunition, is currently pending ratification at the United Nations. Same is expected to shortly be ratified by some 153 countries including the U.S.

221. In The Bahamas, the excessive accumulation and uncontrolled infiltration of small arms and light weapons continues to present a significant challenge to law enforcement agencies and by extension to national security. The availability of illegal firearms has contributed to an escalation in serious crimes including murder, armed robbery, armed conflicts, gang violence, house breakings, and organized crime.

222. Proceeds derived trafficking in firearms is a predicate offence under the POCA, as amended with the attendant penalties.
FRAUD

223. Fraud is a false representation of a matter of fact whether by words or by conduct, by false or misleading allegations, or by concealment of what should have been disclosed that deceives and is intended to deceive another so that the individual will act upon it to her or his legal injury. Put otherwise, fraud is dishonesty calculated for advantage or profit. Because of the link between fraud and money laundering, it is important that such matters are reported to the FIU.

224. To establish fraud, it must be proved that the defendant's actions involved:
(a) a false statement of a material fact;
(b) knowledge on the part of the defendant that the statement is untrue;
(c) intent on the part of the defendant to deceive the alleged victim;
(d) justifiable reliance by the alleged victim on the statement; and
(e) injury to the alleged victim as a result.

225. In The Bahamas, where a person or entity is convicted of fraud by the Courts, judgment has generally taken the form of fines, prison sentences, an Order for Restitution to the victim(s) or a combination of same.

226. Fraud is often perceived to be a victimless crime. In reality it presents risks to individuals, businesses and institutions as well as the government. Aside from the direct financial loss, fraud places a severe emotional strain on individuals, their families and friends, and at a macro level, can damage The Bahamas' international reputation as a safe place to do business and can impact public confidence in the services offered by the public, private and voluntary sectors.

227. It is not possible to identify the overall level of organised criminal activity locally against each fraud type or victim, as not all cases of fraud are reported. However, very few areas of everyday life have not been impacted by fraud, which can be broadly classified into four general categories, each of which has many subcategories:

(a) Individual Fraud: - Any fraud that targets an individual directly, e.g. advance fee fraud, miracle health scams, ponzi schemes, pyramid schemes. Individual frauds can differ from frauds affecting businesses and other organizations;

(b) Corporate Fraud: - Any fraud committed against a business e.g. cheque frauds, false accounting frauds, insurance frauds, pilferage, travel and subsistence fraud. Fraud impacting businesses can be both general frauds that target any business to sector specific frauds;
(c) **On-Line Fraud:** This fraud is perpetrated primarily via the internet, e.g. charity donation frauds, inheritance frauds, lottery scams and plastic card scams; and

(d) **Advance Fee Fraud:** The fraudster targets victim to make advance or up-front payment for goods, services and/or financial gains that do not materialize, e.g. career opportunity scams, psychic scams, impersonation of officials, West African Letters Scams.

228. **HUMAN SMUGGLING**

229. **People smuggling** (also called people or **human smuggling**) is a form of transnational organized crime. It is the facilitation, transportation, attempted transportation or illegal entry of a person or persons across an international border, in violation of one or more countries laws, either clandestinely or through deception, such as the use of fraudulent documents. The term is understood as and often used interchangeably with **migrant smuggling**, which is defined by the United Nations Convention Against Transnational Organized Crime also known as the ‘**Palermo Convention**’ of 2004. The Bahamas is a signatory to this Convention.

230. Human smuggling is a secretive, illicit activity, and one that is increasingly controlled by transnational organized crime syndicates, due to significant financial gains attached. The Bahamas is affected by people smuggling, be it in the capacity of country of origin, transit, or destination via periodic apprehensions of person of various nationalities inside and external to the region.

231. This activity, specifically migrant smuggling, constitutes ‘criminal conduct’ under the Proceeds of Crime Act, 2000, as amended and Section 47 of the Immigration Act. A significant contributing factor behind the success of smuggling operations comes from the participation of both local citizens and foreign nationals in this activity which keeps law enforcement on constant alert.

232. Human smuggling can generate substantial profits for those involved, which in turn can fuel corruption and organized crime in countries traveled from, through, or to during the smuggling process. Smugglers’ fees vary from destination to destination, but on the whole, they have risen dramatically over the years. A 2009 estimate placed the human smuggling business at $20 Billion annually.
233. As, opportunities to migrate legally are severely limited, migrants, including asylum seekers, have increasingly resorted to illegal entry and unauthorized stays, and ever-larger numbers use the services of smugglers to evade the system, compounding their vulnerability to exploitation and in some cases certain death.

**LOTTERIES**

234. The regulation of lotteries and casino gaming and all matters connected therewith, or incidental thereto, are governed by the *Lotteries and Gaming Act*.

235. The modern day lottery is perceived to be a form of ‘gambling’ that offers substantial financial payouts to the winner(s) but generally appears to have certain basic characteristics, namely:

(a) a sizable pool or population of willing participants commonly referred to as ‘bettors;’
(b) each bettor buys a receipt or writes down his / her number choices to be entered into the pool; Bettors are also able to place their bets online in the comfort and privacy of their homes, workplace, number houses, or wherever they may be, by the click of a mouse of a computer, or the use of a mobile device.
(c) a drawing by various means is held and a winner(s) identified;
(d) the value of the prize(s) given is the amount remaining after deducting operating expenses;
(e) depending upon jurisdiction, winnings may be subject to taxes.

236. In some countries e.g. US, Canada, UK, Europe, South Africa, Australia, New Zealand., governments seeking to raise revenues for various civic programs have instituted officially sanctioned independently audited or national lotteries. In The Bahamas, there is no national or state sanctioned lottery as such, as all lotteries are illegal pursuant to *Section 3 of the Act*.

237. In the absence of a national lottery, many residents and other interested parties participate in foreign based lotteries largely via the internet. Alternatively, others participate in unsanctioned games of chance offered by local business establishments referred to as ‘number houses.’ Winning receipts or numbers are announced daily. In case of foreign lotteries, winning numbers are announced in the print and electronic media, whereas local businesses make their announcements via informal channels with payouts being made in cash or credited to in-house accounts maintained by the bettors.

238. Since all lotteries are illegal, as per Section 3 of the Act, all winnings received by Bahamian citizens or local residents from participating in foreign lotteries or local numbers houses are subject to seizure and
forfeiture under the **Lotteries and Gaming Act.**

**NON PROFIT ORGANIZATIONS**

239. Non-profit organizations (NPOs) are defined by their purpose, their reliance on contributions from supporters and the trust placed in them by the wider community. They may often process large amounts of cash and regularly transmit funds between jurisdictions. In practice, based on their purpose, NPOs may fall under a number of categories including charitable, educational, scientific, political, religious, literary, artistic, etc.

240. Non-profit organizations in The Bahamas are captured under Sections 161 to 169 of the **Companies Act, as amended.** Section 161 stipulates that the memorandum of a non-profit company shall state:

   (a) the restrictions on the undertaking that the company is to carry on;
   (b) that the company has no authorized share capital and is to be carried on without pecuniary gain to its members and that any profits or other accretions to the company are to be used in furthering its undertaking;
   (c) if the undertaking of the company is of a social nature the address in full of the club house or similar building maintained by the company; and
   (d) that each first director becomes a member of the company upon its incorporation.

241. Concerns about the possible misuse of NGOs for purpose of money laundering and financing of terrorism is reflected by their inclusion in the **FATF’s Recommendation (Recommendation 8)** for special attention by all countries.

242. Such misuse could possibly occur in several ways:

   1) by re-directing NPO generated funds to terrorist rather than to altruistic means and the laundering of money to provide legitimate means of transmission of funds between multiple jurisdictions;
   2) assets such as vehicles and property could be used to transport or house operatives, money and weapons, and provide relatively safe places where members can meet;
   3) the NPO may simultaneously provide overt humanitarian aid for legitimate causes and covertly provide succor to terrorist activities;
   4) while properly registered and fully compliant with requisite regulatory requirements, the NPO may be used as a front for laundering of money, or appropriation of terrorism funds or for the rallying support for terrorist activities.

**SCAMS**

243. Such schemes continue to surface with the ultimate objective being to try and separate unsuspecting individuals or businesses from their money or
property. Methods employed in such endeavors would appear to be limited only by resourcefulness and creativity of the criminal elements and in some instances are multi jurisdictional in scope. Schemes which have surfaced locally include: e-mails, investments with guaranteed returns; front end fees; real estate sales/development; cheque fraud; counterfeit currency; pyramids; misappropriation of inventory; stealing by reason of employment/service; etc.

**TAX EVASION**

244. Generally defined, ‘tax evasion’ is the criminal non-payment of legitimate tax liabilities (i.e. revenue), due to the state by both corporate and individual tax payers in that state. In most countries today, tax evasion is classified as criminal conduct. Such activity is punishable either by fines, imprisonment or both, as the decline in tax revenues through the use of international tax planning and other initiatives have become a major concern for affected governments.

245. Since 2009, there has been a growing consensus for improving transparency and international cooperation, to counter offshore tax evasion, led by the OECD’s Global Forum. This oversight by the Global Forum has resulted in the implementation of standards of transparency and exchange of information for tax purposes. Such standards require countries to put in place appropriate legal and regulatory framework for transparency and to facilitate exchange of information.

246. Tax Information Exchange Agreements or TIEAs are bilateral agreements by which countries make arrangements to cooperate for the exchange of information in relation to tax matters. Signed agreements enter into force only when the necessary internal procedures have been completed. The effective date of an agreement depends on the specific provision contained in the agreement.

247. The Bahamas has entered into thirty (30) tax information exchange agreements (TIEAs), since January 2002, and has implemented enabling legislation in the form of the **International Tax Cooperation Act**, which was passed on 1st July 2010. As such, The Bahamas has taken all steps which are necessary on its part to bring all of its TIEAs into force and thereby demonstrate its commitment to the global effort to eliminate tax evasion.

248. In its **2011 Phase 1 Peer Review Report** on The Bahamas, The OECD’s Global Forum has confirmed The Bahamas status as compliant.
TRAFFICKING IN PERSONS

249. Trafficking in persons is a serious crime and a grave violation of human rights. The war against terrorism, narcotics, and irregular migration has moved this issue up the international policy agenda.

250. Article 3 (a) of the UN Protocol to Prevent, Suppress and Punish Trafficking in Persons defines Trafficking in Persons as the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs.

251. Every year, thousands of men, women and children fall into the hands of traffickers, in their own countries and abroad. Almost every country in the world is affected by trafficking, whether as a country of origin, transit or destination for victims.

252. The list of offences under The Trafficking in Persons (Prevention and Suppression) Act, 2008 constitutes ‘criminal conduct’ under the Proceeds of Crime Act, 2000, as amended.

VALUE ADDED TAX (VAT)

253. The 2012/2013 Budget included a provision by the Central Government for the introduction of a Value Added Tax (VAT), effective 1st July 2014 to assist in broadening the country’s tax base. The introduction of the new tax is intended to offset the eventual reduction in import duty rates that will accompany The Bahamas’ accession to the World Trade Organization and assist in consolidating the country’s finances. Under the new regime, a 15% VAT rate will be applied to a broad range of goods and services while a number of other categories will be exempted.

WEAPONS OF MASS DESTRUCTION

254. “Weapon of Mass Destruction” (WMD) is a term used to characterize a variety of weapons that share two key features: their potential for large-scale destruction and the indiscriminate nature of their effects, notably against civilians. There are three major types of WMD: nuclear weapons, chemical warfare agents, and biological warfare agents. In addition, some analysts include radiological weapons as a fourth category.
FATF’s Recommendation 7 mandates all countries to implement targeted financial sanctions to prevent, suppress and disrupt the proliferation of weapons of mass destruction and its financing. These initiatives require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.

Many countries already possess WMDs, or have the capacity to produce them, while an increasing number are in the process of acquiring and developing capabilities to inflict mass casualties and destruction. While many terrorist groups lack the resources or expertise to employ WMD, there has been a growing interest among certain terrorist groups in acquiring such weapons. The serious issue of proliferation of these weapons has become an urgent matter that many governments are attempting to address.

Recommendation 7 has been implemented in The Bahamas via the International Obligations (Economic and Ancillary Measures) Act, 1993 which provides for the imposition of economic sanctions and the taking of ancillary measures to give effect to the international obligations of The Bahamas. Where an offence under this Act is committed by a body corporate and it is proved that such offence was committed with the consent or connivance of or is attributable to any neglect on the part of any director, manager, secretary or other officer of the body corporate or any person purporting to act in such capacity, then he as well as the body corporate shall be deemed to be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

**XXI - MONEY LAUNDERING AND FINANCING OF TERRORISM OFFENCES, PENALTIES AND DEFENCES**

Proceeds of Crime Act, 2000, as Amended:

**Concealing or Dealing with the Proceeds of Criminal Conduct**

It is an offence to use, transfer, send or deliver to any person or place, or to dispose of, convert, alter or otherwise deal with any property, for the purpose of concealing or disguising such property, knowing, suspecting or having a reasonable suspicion that the property (in whole or in part, directly or indirectly) is the proceeds of criminal conduct. For this offence, references to concealing or disguising property includes concealing or disguising the nature, source, location, disposition, movement or ownership or any rights with respect to the property. This section applies to a person’s
own proceeds of criminal conduct or where he knows or has reasonable grounds to suspect that the property he is dealing with represents the proceeds of another’s criminal conduct.

259.1. **Penalty**: On summary conviction to five years imprisonment or a fine of $100,000.00 or both; or on conviction on information to imprisonment for twenty years or to an unlimited fine or both.

**Assisting Another to Conceal the Proceeds of Criminal Conduct**

260. It is an offence for any person to provide assistance to a criminal for the purpose of obtaining, concealing, retaining or investing funds, knowing or suspecting, or having reasonable grounds to suspect that those funds are the proceeds of criminal conduct or any relevant offence.

260.1 **Penalty**: On summary conviction to five years imprisonment or a fine of $100,000.00 or both; or on conviction on information to imprisonment for twenty years or to an unlimited fine or both.

260.2 **Defence**: It is a defence that the person concerned did not know, suspect or have reasonable grounds to suspect that the funds in question are the proceeds of criminal conduct, or that he intended to disclose to a police officer his suspicion, belief or any matter on which such suspicion or belief is based, but there is a reasonable excuse for his failure to make a disclosure.

**Acquisition, Possession or Use**

261. It is an offence to acquire, use or possess property which are the proceeds (whether wholly or partially, directly or indirectly) of criminal conduct, knowing, suspecting or having reasonable grounds to suspect that such property are the proceeds of criminal conduct. Having possession is construed to include doing any act in relation to the property.

261.1 **Penalty**: On summary conviction to five years imprisonment or a fine of $100,000.00 or both; or on conviction on information to imprisonment for twenty years or to an unlimited fine or both.

261.2 **Defence**: It is a defence that the property in question was obtained for adequate consideration. [NB: The provision for any person of goods or services which assist in the criminal conduct does not qualify as consideration for the purposes of this offence.]

**Failure to Disclose**

262. It is an offence if a person 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 and fails to disclose or report that transaction or proposed transaction to the Financial Intelligence Unit or to a police officer, as soon as practicable after forming that suspicion, if the information or the matter on which the information is based came to his attention in the course of his trade, profession, business or employment.
261.1 **Penalty:** On summary conviction to three years imprisonment or a fine of $50,000.00 or both; or on conviction on information, to imprisonment for ten years or to an unlimited fine or both.

261.2 **Defense:** It is a defense to prove that the defendant took all reasonable steps to ensure that he complied with the statutory requirement to report a transaction or proposed transaction; or that in the circumstances of the particular case, he could not reasonably have been expected to comply with the provision.

261.3 In the case of a person who is employed by a financial institution, internal reporting in accordance with the procedures laid down by the employer, pursuant to the Financial Intelligence (Transactions Reporting) Regulations, 2001, as amended, will satisfy the requirement to report suspicious transactions. The Financial Transactions Reporting Act, 2000, as amended, and The Financial Intelligence Unit Act, 2000, as amended, protects those financial institutions reporting suspicions of money laundering from claims in respect of any alleged breach of client confidentiality.

**Financial Transactions Reporting Act, 2000, as Amended:**

**Suspicion**

262. Section 14 of the Financial Transactions Reporting Act provides that financial institutions that know, suspect or have reasonable grounds to suspect that the transaction or proposed transaction involves proceeds of criminal conduct as defined in the Proceeds of Crime Act, 2000, as amended, or any offence under the Proceeds of Crime Act, 2000, as amended or an attempt to avoid the enforcement of any provision of the Proceeds of Crime Act, 2000, as amended, shall, as soon as practicable after forming that suspicion, make a report to the Financial Intelligence Unit.

262.1 A Suspicious Transaction Report (STR) should be made in writing, and should contain the necessary requirements in accordance with the Act. However, where the urgency of the situation requires it, the STR may be made orally to the Financial Intelligence Unit. As soon as possible thereafter, a report that complies with the legislation should be forwarded. Failure to report a Suspicious Transaction may result in a penalty.

262.2 **Penalty:** On summary conviction for an individual, to a fine not exceeding $20,000.00, or in the case of a body corporate, $100,000.00.

**Tipping Off – Suspected Party**

263. It is also an offence for anyone who knows suspects or has reasonable grounds to suspect that a disclosure has been made to a police officer or appropriate person, or that the authorities are acting, or are proposing to act, in connection with an investigation into money laundering, to prejudice an investigation by so informing the person who is the subject of a suspicion, or any third party of the disclosure, action or proposed action.

263.1 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 a suspicious transaction report 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.

263.2 Where it is known or suspected that a suspicious transaction report has already been disclosed to the Financial Intelligence Unit, the Police or other authorized agency and it becomes necessary to make further enquiries, persons within the disclosing institution should take great care to ensure that customers do not become aware that their names have been brought to the attention of the authorities.

263.3 **Penalty:** On summary conviction to a term of three years imprisonment or a fine of $50,000.00 or both; on conviction on information the penalty is a term of ten years imprisonment or an unlimited fine or both.

263.4 **Defence:** It is a defence if the person making the disclosure proves he did not know or suspect that the disclosure was likely to prejudice the investigation, or that the disclosure was made under a lawful authority or with reasonable excuse.

**Tipping Off – Third Party**

263.5 It is an offence for a person who is an employee of a financial institution, or having become aware, in the course of their duties as an employee or agent, that the police is or may be conducting an investigation into any transaction or proposed transaction of an STR and knowing that he is not legally authorized to disclose the information, knowingly discloses that information to any other person, to obtain an advantage or a pecuniary gain or to prejudice the investigation.

263.6 **Penalty:** On summary conviction in the case of an individual to a fine not exceeding $5,000.00 or to imprisonment for a term not exceeding six months and in the case of a body corporate to a fine not exceeding $20,000.00

263.7 **Defence:** It shall be a defence if he took all reasonable steps to ensure that he complied with these provisions, or could not reasonably have been expected to comply.

**Anti-Terrorism Act, 2004**

**The Offence of Terrorism**

264. **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) substantial damage to property; or
(iv) which causes serious interference with or serious disruption of an essential service, facility or system.

264.1 **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**

265. **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**

266. **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 suspected 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 of the financial services were used to carry out the offence.

266.1 **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**

267. **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.

**Penalty:** On conviction on information the penalty is a fine of $2,000,000.00.
Investigation

Section 7(1) 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. (In the case of a financial institution, such a report must be made to the Financial Intelligence Unit, as per amendment to Schedule 2 of the Financial Intelligence Unit Act, 2000), as amended.

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 suspected 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 suspicions 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 the 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 the Act.

XXII - EXAMPLES OF TERRORIST FINANCING

This Section provides some examples, based on genuine cases, of how individuals and organizations might raise and use monies and other financial instruments to finance terrorism. These are intended to help
financial services businesses to recognize terrorist transactions by identifying some of the most common sources of terrorist funding and business areas which are at a high risk.

(i) Donations
272.1. It is a common practice within the Islamic community to donate a “zakat”, one tenth of one’s income to charity. Other communities also make generous donations to charities. There should be no assumption that such donations bear a relation to terrorist funding. However, donations continue to be a lucrative source of funds from private individuals, rogue states and also from the sale of publications. The latter donations are often made on an irregular basis.

(ii) Extortion
272.2. This form or raising money continues to be one of the most prolific and highly profitable. Monies are usually raised from within the community of protection money. Eventually, extortion becomes a built in cost of running a business within the community.

(iii) Smuggling of Goods
272.3. Smuggling across a border has become one of the most profitable ventures open to terrorist organizations. Smuggling requires a co-coordinated, organized structure, with a distribution network to sell the smuggled goods. Once set up, the structure offers high returns for low risks. Criminal partners benefit from their involvement and considerable amounts are often made available for the terrorist organization.

272.3A. The profits are often channeled via couriers to another jurisdiction. The money frequently enters the banking system by the use of front companies and there have been instances of the creation of specialized bureau de change facilities, whose sole purpose is to aid in the laundering of the proceeds of smuggling.

272.3B. In addition, the smuggler sometimes gives monies to legitimate businesses which are not associated with the smuggling operation. These monies are paid into the banking system as part of a company’s normal turnover. Provided the individuals are not greedy, detection is extremely difficult.

(iv) Charities
272.4. There are known cases of charities being used to raise funds for the sole purpose of terrorist activities. In some cases, charities have strayed outside the legal remit for which they were originally formed or they have not always published full accounts of the projects, which their fund raising has helped to finance.

(v) Drugs
272.5. The provision of drugs can be highly profitable source of funds and is used by some groups to finance other criminal activities. Many terrorist groups are not directly involved in the importation or distribution, but in order for
the drug suppliers to operate within a certain area or community, a levy would have to be paid. Such extortion, often known as protection money, is far less risky than being responsible for organizing the supply and distribution of drugs.

(vi) Counterfeit Goods

272.6. Increasingly, counterfeiting is being used to fund terrorist organizations. Interpol is of the opinion that counterfeit goods can be linked to most terrorist organizations, including Al Qaeda, and has the potential to become the preferred source of income. The International Chamber of Commerce estimates that counterfeit goods accounted for 6% of world trade in 2003 with an estimated value of around £260 billion.
INTERNATIONAL CONVENTIONS

I. THE FATF REVISED RECOMMENDATIONS

Paris, 16 February 2012

Money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction are serious threats to security and the integrity of the financial system.

The FATF Standards have been revised to strengthen global safeguards and further protect the integrity of the financial system by providing governments with stronger tools to take action against financial crime. At the same time, these new standards will address new priority areas such as corruption and tax crimes.

The revision of the Recommendations aims at achieving a balance:

- On the one hand, the requirements have been specifically strengthened in areas which are higher risk or where implementation could be enhanced. They have been expanded to deal with new threats such as the financing of proliferation of weapons of mass destruction, and to be clearer on transparency and tougher on corruption.

- On the other, they are also better targeted – there is more flexibility for simplified measures to be applied in low risk areas. This risk-based approach will allow financial institutions and other designated sectors to apply their resources to higher risk areas.

- The FATF Recommendations are the basis on which all countries should meet the shared objective of tackling money laundering, terrorist financing and the financing of proliferation. The FATF calls upon all countries to effectively implement these measures in their national systems.

THE FATF RECOMMENDATIONS

A. AML/CFT POLICIES AND COORDINATION

1. Assessing risks and applying a risk-based approach *

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority
or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.

Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

2. National cooperation and coordination

Countries should have national AML/CFT policies, informed by the risks identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies.

Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policy-making and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

B. MONEY LAUNDERING AND CONFISCATION

3. Money laundering offence *

Countries should criminalize money laundering on the basis of the Vienna Convention and the Palermo Convention. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences.

4. Confiscation and provisional measures *

Countries should adopt measures similar to those set forth in the Vienna Convention, the Palermo Convention, and the Terrorist Financing Convention, including legislative measures, to enable their competent authorities to freeze or seize and confiscate the following, without prejudiceing the rights of bona fide third parties: (a) property laundered, (b) proceeds from, or instrumentalities used in or intended for use in money laundering or predicate offences, (c) property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organizations, or (d) property of corresponding value.

Such measures should include the authority to: (a) identify, trace and evaluate property that is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the country’s ability to freeze or seize or recover property that is
subject to confiscation; and (d) take any appropriate investigative measures.

C. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

5. Terrorist financing offence *

Countries should criminalize terrorist financing on the basis of the Terrorist Financing Convention, and should criminalize not only the financing of terrorist acts but also the financing of terrorist organizations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicate offences.

6. Targeted financial sanctions related to terrorism and terrorist financing *

Countries should implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to resolution 1373 (2001).

7. Targeted financial sanctions related to proliferation *

Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.

8. Non-profit organizations *

Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organizations are particularly vulnerable, and countries should ensure that they cannot be misused:

(a) by terrorist organizations posing as legitimate entities;
(b) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and
(c) to conceal or obscure the clandestine diversion of funds intended for legitimate
purposes to terrorist organizations.

D. PREVENTIVE MEASURES

9. Financial institution secrecy laws

Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

CUSTOMER DUE DILIGENCE AND RECORD-KEEPING

10. Customer due diligence *

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names. Financial institutions should be required to undertake customer due diligence (CDD) measures when:

(i) establishing business relations;
(ii) carrying out occasional transactions: (a) above the applicable designated threshold (USD/EUR 15,000); or (b) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;
(iii) there is a suspicion of money laundering or terrorist financing; or
(iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The principle that financial institutions should conduct CDD should be set out in law.

These requirements should apply to all new customers, although financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.

11. Record-keeping

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should be required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.
ADDITIONAL MEASURES FOR SPECIFIC CUSTOMERS AND ACTIVITIES

12. Politically exposed persons *

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

(a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
(b) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
(c) take reasonable measures to establish the source of wealth and source of funds; and
(d) conduct enhanced ongoing monitoring of the business relationship.

Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d).

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

13. Correspondent banking *

Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to:

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent’s business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;
(b) assess the respondent institution’s AML/CFT controls;
(c) obtain approval from senior management before establishing new correspondent relationships;
(d) clearly understand the respective responsibilities of each institution; and
(e) with respect to “payable-through accounts”, be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.

Financial institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks. Financial institutions should be
required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

14. **Money or value transfer services** *

Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions.

15. **New technologies**

Countries and financial institutions should identify and assess the money laundering or 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 or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

16. **Wire transfers** *

Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures.

**RELIANCE, CONTROLS AND FINANCIAL GROUPS**

17. **Reliance on third parties** *

Countries may permit financial institutions to rely on third parties to perform elements of the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

(a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10.
(b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.
(c) The financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11.
(d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

18. **Internal controls and foreign branches and subsidiaries** *

Financial institutions should be required to implement programs against money laundering and terrorist financing. Financial groups should be required to implement group-wide programs against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.

19. **Higher-risk countries** *

Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks.

**REPORTING OF SUSPICIOUS TRANSACTIONS**

20. **Reporting of suspicious transactions** *

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).

21. **Tipping-off and confidentiality**

Financial institutions, their directors, officers and employees should be:

(a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and

(b) prohibited by law from disclosing (“tipping-off”) the fact that a suspicious transaction report (STR) or related information is being filed with the FIU.
DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

22. **DNFBPs: customer due diligence** *

The customer due diligence and record-keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, apply to designated non-financial businesses and professions (DNFBPs) in the following situations:

(a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.

(b) Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate.

(c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

(d) Lawyers, notaries, other independent legal professionals and accountants – when they prepare for or carry out transactions for their client.

23. **DNFBPs: Other measures** *

The requirements set out in Recommendations 18 to 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

(a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d) of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

(b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

(c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to in paragraph (e) of Recommendation 22.

E. **TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS**

24. **Transparency and beneficial ownership of legal persons** *

Countries should take measures to prevent the misuse of legal persons for money laundering or terrorist financing. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares or bearer share warrants, or which allow nominee shareholders or nominee directors, should take effective measures to ensure that they are not misused for money laundering or terrorist financing.
25. **Transparency and beneficial ownership of legal arrangements** *

Countries should take measures to prevent the misuse of legal arrangements for money laundering or terrorist financing. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities.
F. POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES, AND OTHER INSTITUTIONAL MEASURES

REGULATION AND SUPERVISION

26. Regulation and supervision of financial institutions *

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities or financial supervisors should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a financial institution. Countries should not approve the establishment, or continued operation, of shell banks.

At a minimum, where financial institutions provide a service of money or value transfer, or of money or currency changing, they should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements.

27. Powers of supervisors

Supervisors should have adequate powers to supervise or monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorized to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose sanctions, in line with Recommendation 35, for failure to comply with such requirements. Supervisors should have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the financial institution’s license, where applicable.

28. Regulation and supervision of DNFBPs *

Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

(a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary AML/CFT measures.
(b) Countries should ensure that the other categories of DNFBPs are subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements.

The supervisor or SRB should also (a) take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding or being the beneficial owner of a significant or controlling interest or holding a management function, e.g. through evaluating persons on the basis of a “fit and proper” test; and (b) have effective, proportionate, and dissuasive sanctions in line with Recommendation 35 available to deal with failure to comply with AML/CFT requirements.
OPERATIONAL AND LAW ENFORCEMENT

29. Financial intelligence units *

Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

30. Responsibilities of law enforcement and investigative authorities *

Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations within the framework of national AML/CFT policies. At least in all cases related to major proceeds-generating offences, these designated law enforcement authorities should develop a pro-active parallel financial investigation when pursuing money laundering, associated predicate offences and terrorist financing. This should include cases where the associated predicate offence occurs outside their jurisdictions. Countries should ensure that competent authorities have responsibility for expeditiously identifying, tracing and initiating actions to freeze and seize property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime.

31. Powers of law enforcement and investigative authorities

When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions, DNFBPs and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence.

Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing.

32. Cash couriers *

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including through a declaration system and/or disclosure system.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing, money laundering or predicate offences, or that are falsely declared or disclosed.
GENERAL REQUIREMENTS

33. Statistics

Countries should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CFT systems. This should include statistics on the STRs received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for cooperation.

34. Guidance and feedback

The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

SANCTIONS

35. Sanctions

Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons covered by Recommendations 6, and 8 to 23, that fail to comply with AML/CFT requirements. Sanctions should be applicable not only to financial institutions and DNFBPs, but also to their directors and senior management.

G. INTERNATIONAL COOPERATION

36. International instruments

Countries should take immediate steps to become party to and implement fully the Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; and the Terrorist Financing Convention, 1999. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001; the Inter-American Convention against Terrorism, 2002; and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005.

37. Mutual legal assistance

Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions, and related proceedings. Countries should have an adequate legal basis for providing assistance and, where appropriate, should have in place treaties, arrangements or other mechanisms to enhance cooperation.
38. Mutual legal assistance: freezing and confiscation *

Countries should ensure that they have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered; proceeds from money laundering, predicate offences and terrorist financing; instrumentalities used in, or intended for use in, the commission of these offences; or property of corresponding value.

39. Extradition

Countries should constructively and effectively execute extradition requests in relation to money laundering and terrorist financing, without undue delay. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organizations.

40. Other forms of international cooperation *

Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing cooperation. Countries should authorize their competent authorities to use the most efficient means to cooperate. Should a competent authority need bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), these should be negotiated and signed in a timely way with the widest range of foreign counterparts.

Historical versions of the FATF Recommendations


FATF Recommendations - 2003

FATF Recommendations - 1996

FATF Recommendations - 1990

IX Special Recommendations

II. THE UNITED NATIONS’ CONVENTIONS

A number of UN conventions have been developed over the past two decades to deal with prevention of money laundering and terrorist financing. These now include: -

a) the United Nations Convention against Trafficking in Narcotics and Psychotropic Substances (“The Vienna Convention”);

b) the United Nations Convention against Transnational Organized Crime (“The
c) the United Nations Convention against Corruption; and

The Vienna Convention

The “Vienna Convention,” which came into force in November 1990, contains strict obligations. Countries, which become parties to the Vienna Convention, must commit to:

a) criminalize drug trafficking and associated money laundering;
b) enact measures for the confiscation of proceeds of drug trafficking;
c) enact measures to permit international assistance;
d) empower the Courts to order that banks, financial or commercial records are made available to enforcement agencies, regardless of secrecy laws.

The United Nations Convention Against Transnational Organized Crime (The Palermo Convention)

This Convention spells out how countries can improve cooperation on such matters as extradition, mutual legal assistance, transfer of proceedings and joint investigations. It contains provisions for victim and witness protection and shielding legal markets from infiltration by organized criminal groups. Parties to the treaty would also provide technical assistance to developing countries to help them take the necessary measures and upgrade their capacities for dealing with organized crime.

Also adopted by the Assembly are two optional protocols by which countries would undertake in-depth measures to combat smuggling of migrants and the buying and selling of women and children for sexual exploitation or sweat shop labor. A third protocol, dealing with the illicit manufacturing of and trafficking in firearms, is under negotiation.

The third protocol would commit parties to setting controls on the illicit manufacture and sale of firearms, which have been playing an increasing role in civilian violence, terrorism and organized crime.

The United Nations Convention Against Corruption

This Convention attempts to address on a global basis the problems related to corruption. It expands on the provisions of existing regional anti-corruption instruments to prevent corruption and provides channels for governments to recover assets that have been illicitly acquired by corrupt former officials. The Convention also provides for the criminalization of certain corruption related activities such as bribery and money laundering, and for the provision of mutual legal assistance related to those activities.

The United Nations Convention for the Suppression of the Financing of Terrorism
This Convention requires consenting parties to criminalize the provision or collection of funds with the intent that they be used, or in the knowledge that they are being used, to conduct certain terrorist activity. The Convention, inter alia, encourages implementation of measures consistent with the FATF’s Forty Recommendations.

III. UNITED NATIONS RESOLUTIONS

The Security Council of the United Nations has been a driving force in combating the financing of terrorism. In this regard, the following resolutions have been adopted:

I). Resolution 1267 – This Resolution targets specific individuals, entities, or groups, among them Usama Bin Laden, Al-Qaeda and the Taliban, for the purpose of restoring peace and suppressing threats to international security. With respect to the financing of terrorism, its major application is to freeze the assets of the named individuals and entities.

II) Resolution 1373 - This Resolution targets international terrorism in general. It was adopted after the attack of September 11, 2001. The Resolution provides for a set of measures (including the freezing of terrorist assets) aimed at combating terrorism and its financing.

In addition, the UN has been the driving instrument over the years in ongoing efforts to prevent the proliferation of weapons of mass destruction as evidenced by UN Security Council Resolution 1540 (2004) which obliges all States to refrain from providing any form of support to non-state actors that attempt to develop, acquire, manufacture, possess, transport, transfer, or use nuclear, chemical or biological weapon and their means of delivery. All states are to adopt appropriate effective legislation and establish domestic controls to prevent proliferation.

IV  THE UNITED NATIONS ARMS TRADE TREATY (ATT)

The ATT is a multilateral treaty that was negotiated under the auspices of the United Nations in July 2012 in New York, USA. The Treaty regulates the international trade in conventional weapons. The Treaty has not yet entered into force as its ratification by member nations is pending. However, The Bahamas is included among some eighty five nations that have already signed the treaty and eventual approval/ratification is anticipated by all member states. International weapons commerce is estimated to be in the range of US$70 Billion per year. According to law enforcement authorities, firearms appear to be the weapon of choice by criminals in the committing of serious crimes.
MONEY LAUNDERING AND TERRORIST FINANCING
“RED FLAGS”

The following are examples of potentially suspicious activities, or “red flags,” for both money laundering and terrorist financing. Although these lists are not exhaustive, they are provided to assist to financial institutions in recognizing possible money laundering and terrorist financing schemes. Management’s primary focus should be on reporting suspicious activities, rather than on determining whether the transactions are in fact linked to money laundering, terrorist financing, or a particular crime.

The following examples are red flags that, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny should help to determine whether the activity is suspicious or one for which there does not appear to be a reasonable business or legal purpose. The examples listed hereunder are not intended to be exhaustive.

POTENTIALLY SUSPICIOUS ACTIVITY THAT MAY INDICATE MONEY LAUNDERING

Customers Who Provide Insufficient or Suspicious Information

- A customer uses unusual or suspicious identification documentation, which cannot be readily verified or authenticated.
- A business is reluctant, when establishing a new account, to provide complete information about the nature and purpose of its business, anticipated account activity, prior banking relationships, the names of its officers and directors, or information on its business location.
- A customer’s home or business telephone is disconnected.
- The customer’s background differs from that which would be expected on the basis of his or her business activities.
- A customer makes frequent or large transactions and has no record of past or present employment experience.
- A customer is a trust, company, or Private Investment Company, that is reluctant to provide information on controlling parties and underlying beneficiaries. Beneficial owners may hire nominee incorporation services to establish companies and open bank accounts for those companies while shielding the owner’s identity.

Efforts to Avoid Reporting or Record
**Keeping Requirements**

- A customer or group tries to persuade a bank employee not to file required reports or maintain required records.
- A customer is reluctant to provide information needed to file an internal report, in compliance with the requirement of the Financial Transactions reporting Act.
- A customer is reluctant to furnish identification when purchasing negotiable instruments in recordable amounts.
- A business or customer asks to be exempted from KYC and due diligence requirements.
- A person customarily uses the automated teller machine to make several bank deposits below a specified threshold.
- A customer deposits funds into several accounts, usually in amounts of less than $15,000, which are subsequently consolidated into a master account and transferred outside of the country, particularly to or through a location of specific concern (e.g., countries designated by national authorities and Financial Action Task Force [FATF] on Money Laundering as non-cooperative countries and territories).
- A customer accesses a safe deposit box after completing a transaction involving a large withdrawal of currency, or accesses a safe deposit box before making currency deposits structured at or just under $15,000, to evade verification of source of funds or other filing requirements.

**Funds Transfers**

- Many funds transfers are sent in large, round dollar, hundred dollar, or thousand dollar amounts.
- Funds transfer activity occurs to or from one jurisdiction or to or from a high-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer’s business or history.
- Many small, incoming transfers of funds are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer’s business or history.
- Large, incoming funds transfers are received on behalf of a foreign client, with little or no explicit reason.
- Funds transfer activity is unexplained, repetitive, or shows unusual patterns.
- Payments or receipts with no apparent links to legitimate contracts, goods, or services are received.
- Funds transfers are sent or received from the same person to or from different accounts.
- Funds transfers contain limited content and lack related party information.

**Automated Clearing House Transactions**

- Large-value, automated clearinghouse (ACH) transactions are frequently initiated through third-party service providers (TPSP) by originators that are not bank customers and for which the bank has no or insufficient due diligence.
- TPSP have a history of violating ACH network rules or generating illegal transactions, or processing manipulated or fraudulent transactions on behalf of their customers.

**Activity Inconsistent with the Customer’s Business**

- The currency transaction patterns of a business show a sudden change inconsistent with normal activities.
- A large volume of cashier’s checks, money orders, or funds transfers is deposited into, or purchased through, an account when the nature of the account holder’s business would not appear to justify such activity.
- A retail business has dramatically different patterns of currency deposits from similar businesses in the same general location.
- Unusual transfers of funds occur among related accounts or among accounts that involve the same or related principals.
- The owner of both a retail business and a check-cashing service does not ask for currency when depositing checks, possibly indicating the availability of another source of currency.
- Goods or services purchased by the business do not match the customer’s stated line of business.

**Other Suspicious Customer Activity**

- A customer frequently exchanges small-dollar denominations for large-dollar denominations.
- A customer frequently deposits currency wrapped in currency straps or currency wrapped in rubber bands that is disorganized and does not balance when counted.
- A customer purchases a number of cashier’s checks, money orders, or traveler’s checks for large amounts under a specified threshold.
- A customer purchases a number of open-end stored value cards for large amounts. Purchases of stored value cards are not commensurate with normal business activities.
- A customer receives large and frequent deposits from on-line payments systems, yet has no apparent on-line or auction business.
- Monetary instruments deposited by mail are numbered sequentially or have unusual symbols or stamps on them.
- Suspicious movements of funds occur from one bank to another, and then funds are moved back to the first bank.
- Deposits are structured through multiple branches of the same bank or by groups of people who enter a single branch at the same time.
- Currency is deposited or withdrawn in amounts just below identification or reporting thresholds.
- The customer may visit a safe deposit box or use a safe custody account on an unusually frequent basis.
- Safe deposit boxes or safe custody accounts may be opened by individuals who do not reside or work in the institution’s service area despite the availability of such services at an institution closer to them.
- Unusual traffic patterns in the safe deposit box area or unusual use of safe custody accounts. For example, more individuals may enter, enter more frequently, or carry bags or other containers that could conceal large amounts of currency, monetary instruments, or small valuable items.
- A customer rents multiple safe deposit boxes to store large amounts of currency, monetary instruments, or high-value assets awaiting conversion to foreign currency, for placement into the banking system.
- A customer establishes multiple safe custody accounts to store large amounts of securities awaiting sale and conversion into currency, monetary instruments, outgoing funds transfers, or a combination thereof, for placement into the banking system.
- Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.
- To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via currency or multiple monetary instruments.

**Changes in Bank-to-Bank Transactions**

- The size and frequency of currency deposits increases rapidly with no corresponding increase in non-currency deposits.
- A bank is unable to track the true account holder of correspondent or concentration account transactions.
- The turnover in large-denomination bills is significant and appears uncharacteristic, given the bank’s location.
- Changes in currency-shipment patterns between correspondent banks are significant.

**Trade Finance**

- Transport documents do not match letter of credit documents and evidence an over-shipment or under-shipment not covered by the letter of credit agreement.
- Shipment locations of the goods, shipping terms, or descriptions of the goods are inconsistent with the letter of credit. This may include changes in shipment locations to high-risk countries or changes in the quality of the goods shipped.
- Sudden and unexplained increases in a customer’s normal trade transactions.
- The letter of credit is issued as a bearer instrument or contains unusual clauses or terminology.
- Customers are conducting business in high-risk jurisdictions or geographic locations, particularly when shipping items through high-risk or FATF designated non-cooperative countries.
- Customers involved in potentially high-risk activities (e.g., dealers in weapons, nuclear materials, chemicals, precious gems; or certain natural resources such as metals, ore, and crude oil).
- Obvious over- or under-pricing of goods and services (e.g., importer pays $400 an item for one shipment and $750 for an identical item in the next shipment; exporter charges one customer $100 per item and another customer $400 for an identical item in the same week).
• Excessively amended letters of credit without reasonable justification.
• Transactions evidently designed to evade legal restrictions, including evasion of necessary government licensing requirements.

**Privately Owned Automated Teller Machines**

• Automated teller machine (ATM) activity levels are high in comparison with other privately owned or bank-owned ATMs in comparable geographic and demographic locations.
• Sources of currency for the ATM cannot be identified or confirmed through withdrawals from account, armored car contracts, lending arrangements, or other appropriate documentation.

**Insurance**

• A customer purchases products with termination features without concern for the product’s investment performance.
• A customer purchases insurance products using a single, large premium payment, particularly when payment is made through unusual methods such as currency or currency equivalents.
• A customer purchases product that appears outside the customer’s normal range of financial wealth or estate planning needs.
• A customer borrows against the cash surrender value of permanent life insurance policies, particularly when payments are made to apparently unrelated third parties.
• Policies are purchased that allow for the transfer of beneficial ownership interests without the knowledge and consent of the insurance issuer. This would include secondhand endowment and bearer insurance policies.
• A customer is known to purchase several insurance products and uses the proceeds from an early policy surrender to purchase other financial assets.

**Company Account Activity**

• A bank is unable to obtain sufficient information or information is unavailable to positively identify originators or beneficiaries of accounts or other banking activity (using Internet, commercial database searches, or direct inquiries to a respondent bank).
• Payments have no stated purpose, do not reference goods or services, or identify only a contract or invoice number.
• Goods or services, if identified, do not match the profile of company provided by respondent bank or character of the financial activity; a company references remarkably dissimilar goods and services in related funds transfers; explanation given by foreign respondent bank is inconsistent with observed funds transfer activity.
• Transacting businesses share the same address, provide only a registered agent’s address, or have other address inconsistencies.
• Unusually large number and variety of beneficiaries are receiving funds transfers from one company.
• Frequent involvement of multiple jurisdictions or beneficiaries located in high-risk jurisdictions.
• Use of nested correspondent banking relationships.
Embassy and Foreign Consulate Accounts

- Official embassy business is conducted through personal accounts.
- Account activity is not consistent with the purpose of the account, such as pouch activity or payable upon proper identification transactions.
- Accounts are funded through substantial currency transactions.
- Accounts directly fund personal expenses of foreign nationals without appropriate controls, including, but not limited to, expenses for college students.

Employees

- An employee has a lavish lifestyle that cannot be supported by his or her salary.
- An employee fails to conform to recognized policies, procedures, and processes, particularly in private banking.
- An employee is reluctant to take a vacation.

Potentially Suspicious Activity That May Indicate Terrorist Financing

The following are examples of potentially suspicious activity provided by the FATF. The FATF is an intergovernmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing.

Activity Inconsistent with the Customer’s Business

- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from high-risk countries (e.g., countries designated by national authorities and FATF as non-cooperative countries and territories).
- The stated occupation of the customer is not commensurate with the type or level of activity.
- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
- Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

Funds Transfers

- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves a high-risk jurisdiction.
• Funds transfers sent to the same individual or entity by a client with no obvious concern for the higher service fees.
• Fund transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
• Fund transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, in situations when the inclusion of such information would be expected.
• Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
• Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to high-risk countries.

**Other Transactions That Appear Unusual or Suspicious**

• Transactions involving foreign currency exchanges are followed within a short time by funds transfers to high-risk jurisdictions.
• Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in high-risk jurisdictions.
• A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from high-risk locations when there appear to be no logical business reasons for dealing with those locations.
• Banks from high-risk jurisdictions open accounts.
• Funds are sent or received via international transfers from or to high-risk locations.
• Insurance policy loans or policy surrender values, which are subject to a substantial surrender charge.

**APPENDIX C**

**SUSPICIOUS TRANSACTIONS INDICATORS**

The examples utilized in this section and other parts of these Guidelines are primarily expressed in dollars. However, this does not preclude or detract from the
SECTION A: BANKING

For the purpose of these Guidelines, banking institutions are those financial institutions, which are licensed by the Central Bank of The Bahamas under the Bank and Trust Companies Regulations Act, 2000, as amended.

Vigilance should govern all the stages of the bank’s dealings with the customers, including:

- account opening;
- non-account holding customers;
- safe custody and safe deposit boxes;
- deposit-taking;
- lending;
- transactions into and out of accounts generally, including by way of electronic transfer (wire transfer);
- marketing and self-promotion and.
- Instructions given to financial institutions via telephone, email or other electronic means.

Account opening

In the absence of a satisfactory explanation, the following should be regarded as suspicious customers:

- a customer who is reluctant to provide normal information or who provides only minimal, false or misleading information;
- a customer who provides information, which is difficult or expensive for the bank to verify; and
- a customer who opens an account with a significant cash balance.

Non-account holding customers

Banks, which undertake transactions with persons who are not account holders with them, should be particularly careful to treat such persons (and any underlying beneficial owners of them) as verification subjects.

Safe custody and safe deposit boxes

Particular precautions need to be taken in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such facilities are made available to non-account holders, the strict verification procedures should be followed.

Deposit taking

In the absence of a satisfactory explanation, the following should be regarded as suspicious transactions:

- substantial cash deposits, singly or in accumulations, particularly when:
i. the business in which the customer is engaged would normally be conducted not in cash or in such amounts of cash, but by cheques, bankers’ drafts, letters of credit, bills of exchange, or other instruments; or
ii. such a deposit appears to be credited to an account only for the purpose of supporting the customer’s order for a bankers’ draft, money transfer or other negotiable or readily marketable money instrument; or
iii. deposits are received by other banks and the bank is aware of a regular consolidation of funds from such account prior to a request for onward transmission of funds.

- the avoidance by the customer or its representatives of direct physical contact with the bank;
- the use of nominee accounts, trustee accounts or client accounts which appear to be unnecessary for or inconsistent with the type of business carried on by the underlying customer/beneficiary;
- the use of numerous accounts for no clear commercial reason where fewer would suffice (so serving to disguise the scale of the total cash deposits);
- the use by the customer of numerous individuals (particularly persons whose names do not appear on the mandate for the account) to make deposits;
- frequent insubstantial cash deposits which taken together are substantial;
- frequent switches of funds between accounts in different names or in different jurisdictions;
- matching or payments out with credits paid in by cash on the same or previous day;
- substantial cash withdrawal from a previously dormant or inactive account;
- substantial cash withdrawal from an account which has just received an unexpected large credit from overseas;
- making use of a third party (e.g. a professional firm or a trust company) to deposit cash or negotiable instruments, particularly if these are promptly transferred between client or trust accounts;
- use of better securities outside a recognized dealing system in settlement of an account or otherwise.

**Correspondent banking**

Correspondent banking is the provision of banking services by one bank (the “correspondent bank”) to another bank (the “respondent bank”). Used by banks throughout the world, a correspondent account enables a bank to conduct business and provide services that the bank does not offer directly.

Banks should gather sufficient information about their respondent banks to understand fully the nature of the respondent’s business and guard against holding and/or transmitting money linked to money laundering, corruption, fraud, terrorism or other illegal activity. Factors to consider include: information about the respondent’s bank management, major business activities, where they are located and its anti-money laundering and anti-terrorism prevention and detection initiatives, including their procedures to assess the identity, policies and procedures of any third party entities which will use the correspondent banking services; and the level and robustness of bank regulation and supervision in the
respondent’s country. Banks should only establish correspondent relationships with foreign banks that are effectively supervised by the relevant authorities (paying due regard to the “Non-Cooperative Countries and Territories” as defined by FATF).

Banks should refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (so-called “shell banks”), other high risk banks or with correspondent banks that permit their accounts to be used by shell banks.

Banks should establish that respondent banks have effective customer acceptance and verification policies. Banks, which provide correspondent-banking services to financial services businesses, should also employ enhanced due diligence procedures with respect to transactions conducted through the correspondent accounts.

**Lending**

It needs to be borne in mind that loan and mortgage facilities (including the issuing of credit and charge cards) may be used by launderers at the layering or integration stages. Secured borrowing is an effective method of layering and integration because it puts a legitimate financial business (the lender) with a genuine claim to the security in the way of those seeking to restrain or confiscate the assets.

**Marketing and self-promotion**

In the absence of a satisfactory explanation a customer may be regarded as suspicious if:

- he declines to provide information which would normally make him eligible for valuable credit or other banking services; or
- he makes insufficient use of normal banking facilities, such as higher interest rate facilities for larger credit balances.

**Executorship accounts**

The executors and administrators of an estate should be verified and particular precautions need to be taken when this is not possible.

Payments to named beneficiaries on the instructions of the executors/administrators may be made without further verification. Verification will, however, be required when a beneficiary seeks to transact business in his own name (e.g. setting up a new account).

In the absence of Probate or Letters of Administration to an Estate, persons purporting to be heirs to the estate may attempt to approach the financial institution. In such circumstances, the institution must take all reasonable measures to satisfy itself as to the true identities of any purported heirs to that estate.

**Powers of attorney**
Powers of Attorney and similar third party mandates are often used in The Bahamas for legitimate purposes. However, the same should be regarded as suspicious, if there is no evident reason for granting them. In addition, a wide-ranging scope, excessively used, should also attract suspicion. In any case, verification should be made on the holders of the Powers of Attorney as well as the client and financial services businesses should ascertain the reason for the granting of the Power of Attorney.

**SECTION B: INVESTMENT BUSINESS**

For purpose of these Guidelines, “investment business” refers to financial services businesses, which are licensed by the Securities Commission of The Bahamas under the Investment Funds Act 2003 and the Securities Industry Act, 2011.

**RISK OF EXPLOITATION**

Because the management of investment products is not generally cash based, it is probably less at risk from **placement** of criminal proceeds than is much of the banking sector. Most payments are made by way of cheque or transfer from another financial services business and it can therefore be assumed that in a case of laundering, placement has already been achieved. Nevertheless, the purchase of investments for cash is not unknown, and therefore the risk of investment business used at the **placement stage** cannot be ignored. Payment in cash will therefore need further investigation, particularly where it cannot be supported by evidence of a legitimate cash-based business as the source of funds.

Investment business is likely to be at particular risk to the **layering stage** of money laundering. The liquidity of investment products under management is attractive to launderers since it allows them to quickly and easily move the criminal proceeds from one product to another, mixing them with lawful proceeds and facilitating integration.

Investment business is also at risk to the integration stage in view of:
- the easy opportunity to liquidate investment portfolios containing both lawful and criminal proceeds, while concealing the nature and origins of the latter;
- the wide variety of available investments; and
- the ease of transfer between investment products.

The following investments are particularly at risk:
- collective investment schemes and other “pooled funds” especially where AML/CFT requirements are absent; and
- high risk/high reward products (because the launderer’s cost of funds is by definition low and the potentially high reward accelerates the integration process).

**Borrowing against security of investments**

Secured borrowing is an effective method of layering and integration because it puts a legitimate financial business (the lender) with a genuine claim to the security in the way of those seeking to restrain or confiscate the assets.
Customer’s dealing direct
Where a customer deals with the investment business direct, the customer is the applicant for business to the investment business and accordingly determines who the verification subject(s) is (are). A record should be maintained indicating how the transaction arose and recording details of the paying financial services business’ branch sort code number and account number or other financial services product reference number from which the cheque or payment is drawn.

Intermediaries and underlying customers
Where an agent/intermediary introduces a principal/customer to the investment business and the investment is made in the principal/customer’s name, then principal/customer is the verification subject. For this purpose it is immaterial whether the customer’s own address is given or that of the agent/intermediary.

Nominees
Where an agent/intermediary acts for a customer (whether for a named client or through a client account) but deals in his own name, then the agent/intermediary is a verification subject and the customer is also a verification subject.

Delay in verification
If verification has not been completed within a reasonable time, then the business relationship or significant one-off transaction in question should not proceed any further.

Where an investor exercises cancellation rights, the repayment of money arising in these circumstances (subject to any shortfall deduction where applicable) does not constitute “proceeding further with the business”. However, since this could offer a route for laundering money, investment businesses should be alert to any abnormal exercise of cancellation rights by any investor, or in respect to business introduced through any single authorized intermediary. In the event that abnormal exercise of these rights becomes apparent, the matter should be treated as suspicious and reported through the usual channels. In any case, repayment should not be to a third party.

Redemption prior to completion of verification
Whether a transaction is a significant one-off transaction or is carried out within a business relationship, verification of the customer should normally be completed before the customer receives the proceeds of redemption. However, an investment business will be considered to have taken reasonable measures of verification where payment is made either:
• to the legal owner of the investment by means of a cheque where possible crossed “account payee”; or
• to a bank account held (solely or jointly) in the name of the legal holder of the investment by any electronic means of transferring funds.

Switch transactions
A significant one-off transaction does **not** give rise to a requirement of verification if it is a switch under which all of the proceeds are **directly** reinvested in another investment which itself can, on subsequent resale, only result in either:
- a further reinvestment on behalf of the same customer; or
- a payment being made **directly** to him and of which a record is kept.

### Savings vehicles and regular investment contracts

Except in the case of a small one-off transaction where a customer has:
- agreed to make regular subscriptions or payments to an investment business, and
- arranged for the collection of such subscriptions or payments (e.g. by completing a direct debit mandate or standing order)
the investment business should undertake verification of the customer or satisfy himself that the case is otherwise exempt.

Where a customer sets up a regular savings scheme whereby money invested by him is used to acquire investments to be registered in the name or held to the order of a **third party**, the person who funds the cash transaction is to be treated as the verification subject. When the investment is realized, the person who is then the legal owner (if not the person who funded it) is also to be treated as a verification subject.

### Reinvestment of income

A number of retail savings and investment vehicles offer customers the facility to have income reinvested. The use of such a facility should not be seen as entry into a business relationship; and the reinvestment of income under a facility should not be treated as a transaction, which triggers the requirement of verification.

### Suspicious Transactions

In the absence of satisfactory explanation, the following should be regarded as suspicious transactions:
- introduction by an agent/intermediary in an unregulated or loosely regulated jurisdiction or a sensitive jurisdiction;
- any want of information or delay in the provision of information to enable verification to be completed;
- any transaction involving an undisclosed party;
- early termination, especially at a loss, caused by front-end or rear-end charges or early termination penalties;
- transfer of the benefit of a product to an apparently unrelated third party or assignment of such benefit as collateral;
- payment into the product by an apparently unrelated party; and
- use of bearer securities outside a recognized clearing system, where a scheme accepts securities in lieu of payment.

### SECTION C: TRUST SERVICES

For the purpose of these Guidelines, “trust services” are those services, which are offered to the client by the holder of a trust license issued by the Central Bank of
The Bahamas under the Banks and Trust Companies Regulation Act, 2000, as amended.

Good practice requires key staff to ensure that engagement documentation (client agreement etc.) is duly completed and signed at the time of **entry**.

Verification of new clients should include the following or equivalent steps:

- where a statement is to be made or when accepting trusteeship from a previous trustee or where there are changes to principal beneficiaries, the settlor, and/or where appropriate the principal beneficiary(ies), should be treated as verification subjects;
- in the course of company formation, verification of the identity of underlying beneficial owners;
- where Powers of Attorney and third party mandates are drawn up, verification procedures should deal with both the holders of powers of attorney and the client themselves; new attorneys for corporate or trust business should also be verified; it is always necessary to ascertain the reason for the granting of the Power of Attorney and where there is no obvious reason for granting them, this should be regarded as suspicious; and
- the documentation and information concerning a new client for use by the administrator who will have day-to-day management of the new client’s affairs should include a note of any further required input on verification from any agent/intermediary of the new client, together with a reasonable deadline for the supply of such input, after which suspicion should be considered aroused.

Further to the due diligence undertaken prior to and at the time of commencement of the provision of fiduciary services, the fiduciary has an ongoing obligation to continue to monitor the activities of the entities to which it provides services.

**Suspicious Transactions**

In the absence of any satisfactory explanation, the following should be regarded as suspicious transactions:

- a request for or the discovery of an unnecessarily complicated trust or corporate structure involving several different jurisdictions;
- payments or settlements to or from an administered entity which are of a size or source which had not been expected;
- an administered entity entering into transactions which have little or no obvious purpose or which are unrelated to the anticipated objects;
- transactions involving cash or bearer instruments outside a recognized clearing system, in settlement for an account or otherwise;
- the establishment of an administered entity with no obvious purpose;
- sales invoice values exceeding the known or expected value of goods or services;
- sales or purchases at inflated or undervalued prices;
- a large number of bank accounts or other financial services products all receiving small payments which in total amount to a significant sum;
- large payments of third party cheques endorsed in favor of the customer;
- the use of nominees other than in the normal course of fiduciary business;
• excessive use of wide-ranging Powers of Attorney;
• unwillingness to disclose the source of funds (e.g. sale of property, inheritance, business income etc.);
• the use of postal boxes for no obvious advantage or no obvious necessity,
• tardiness or failure to complete verification;
• administered entities continually making substantial losses;
• unnecessarily complex group structure;
• unexplained subsidiaries;
• frequent turnover of shareholders, directors, trustees, or underlying beneficial owners;
• the use of several currencies for no apparent purposes; and
• arrangements established with the apparent objective of fiscal evasion.

SECTION D: INSURANCE

For the purpose of these Guidelines, “insurance services” are those services provided by insurance entities, which are licensed by the Registrar of Insurance under the Insurance Act, 2005, as amended or the External Insurance Act, 2009.

Insurance business, whether life assurance, pensions or other risk management business, presents a number of opportunities which may involve placing cash in the purchase of a single premium product from an insurer followed by early cancellation and reinvestment.

Surrender prior to completion of verification

Whether a transaction is a significant one-off transaction or is carried out within a business relationship, verification of the customer should be completed before the customer receives the proceeds of surrender. A life insurer will be considered to have taken reasonable measures of verification where payment is made either to:

• the policyholder by means of a cheque, where possible, crossed account payee;
  or
• a bank account held (solely or jointly) in the names of the policyholder by any electronic means of transferring funds.

Switch transactions

A significant one-off transaction does not give rise to a requirement of verification if it is a switch under which all of the proceeds are directly paid to another policy of insurance which itself can, on subsequent surrender, only result in either:

• a further premium payment on behalf of the same customer; or
• a payment being made directly to him and of which a record is kept.

Payments from one policy of insurance to another for the same customer

A number of insurance vehicles offer customers the facility to have payments from one policy of insurance to fund the premium payments to another policy insurance.

The use of such a facility should not be seen as entry into a business relationship and the payments under such a facility should not be treated as a transaction, which triggers the requirement of verification.
Employer-sponsored pension or savings schemes

In all transactions undertaken on behalf of an employer-sponsored pension or savings scheme, the insurer should undertake verification of:

- the principal employer;
- the trustees of the scheme (if any); and
- the members.

Verification of the principal employer should be conducted by the insurer in accordance with the procedures for verification of corporate applicants for business.

Verification of any trustees of the scheme should be conducted and will generally consist of an inspection of the trust documentation:

- the trust deed and/or instrument and any supplementary documentation;
- a memorandum of the names and addresses of current trustees (if any);
- extracts from public registers; and
- references from professional advisers or investment managers.

Verification of members: without personal investment advice

Verification of members is not required by the insurer in respect of a recipient of any payment of benefits made by or on behalf of the employer or trustees (if any) of an employer-sponsored pension or savings scheme if such recipient does not seek personal investment advice.

Verification is required by the insurer, in respect of an individual member of an employer-sponsored pension or savings scheme, if such member seeks personal investment advice, save that verification of the individual member may be treated as having been completed where:

- verification of the principal employer and the trustees of the scheme (if any) has already been completed by the insurer; and
- the principal employer confirms the identity and address of the individual member to the insurer in writing.

Records

The insurer should keep records after termination. In the case of a life company, termination includes the maturity or earlier termination of the policy.

As regards records of transactions, insurers should ensure that they have adequate procedures to access:

- initial proposal documentation including, where these are completed, the client financial assessment (the “fact find”), client needs analysis, copies of regulatory documentation, details of the payment method, illustration of benefits, and copy documentation in support of verification by the insurers;
- all post-sale records associated with the maintenance of the contract, up to and including maturity of the contract; and
- details of the maturity processing and/or claim settlement including completed “discharge documentation.”

In the case of long-term insurance, records usually consist of full documentary evidence gathered by the insurer or on the insurer’s behalf between entry and
termination. If an agency is terminated, responsibility for the integrity of such records rests with the insurer as the product provider.

If an appointed representative of the insurer is itself registered or authorized, the insurer as principal can rely on the representative’s assurance that he will keep records on the insurer’s behalf (it is of course open to the insurer to keep such records itself; in such a case it is important that the division of responsibilities be clearly agreed between the insurer and such representative).

If the appointed representative is not itself so registered or authorized, it is the direct responsibility of the insurer as principal to ensure that, records are kept in respect of the business, that records are kept of the business, that such representative has introduced to it or affected on its behalf.

SUSPICIOUS TRANSACTIONS
In the absence of any satisfactory explanation, the following should be regarded as suspicious transactions:
• application for business from a potential client in a distant place where comparable service could be provided closer to home;
• application for business outside the insurer’s normal pattern of business;
• introduction by an agent/intermediary in an unregulated or loosely regulated jurisdiction or where criminal activity is prevalent;
• any want of information or delay in the provision of information to enable verification to be completed;
• any proposed transaction involving an undisclosed party;
• early termination of a product, especially at a loss caused by front-end loading, or where cash was tendered and/or the refund cheque is payable to a third party;
• “churning” at the client’s request;
• a transfer of the benefit of a product to an apparently unrelated third party;
• use of bearer securities outside a recognized clearing system in settlement of an account or otherwise;
• insurance premiums higher than market levels;
• large, unusual or unverifiable insurance claims;
• unverified reinsurance premiums;
• large introductory commissions; and
• insurance policies for unusual/unlikely exposures.

SECTION E: CASINOS
For the purpose of these Guidelines, casinos are those financial institutions, which are licensed by the Gaming Board of The Bahamas under the Lotteries and Gaming Act, Chapter 387. This Section of the Guidelines contains money laundering typologies which are relevant to licensed casino operators.

(a) Two or more customers purchase chips with currency (e.g., each in excess of $3,000.00, but less than $15,000.00) and then engage in minimal gaming. Subsequently, they combine all of their chips together and one of them goes to the cage and redeems the chips, totaling in excess of $15,000.00, for a casino cheque.
(b) A customer conducts currency transactions (e.g., withdrawals, deposits, redemption of casino chips, etc.), on a regular basis, in amounts that are just under $15,000.00.

(c) A customer pays off a large credit debt, such as markers or bad cheque, of $30,000.00 or more over a short period of time (e.g., less than one week), through a series of currency transactions, none of which exceeds $15,000.00 in a gaming day.

(d) A customer (other than a junket operator known by the casino to be engaged in the business of organizing gambling tours) is observed directly supplying large amounts of currency to individuals who then use the currency for deposit, purchase of chips, exchange of currency, etc.

(e) A customer makes large deposits or pays off large markers (e.g., in excess of $15,000.00) with multiple cashier's cheques, money orders, travelers cheques or other monetary instruments that were issued by several different financial institutions, and none of the instruments is greater than $15,000.00.

(f) A customer withdraws a large amount of funds (e.g., $30,000.00 or more) from a deposit account and requests that multiple casino cheques be issued each of which is less than $15,000.00.

(g) A customer arranges or attempts to arrange large wire transfers out of the country which are paid for by multiple cashier's cheques from different financial institutions in amounts under $15,000.00.

(h) A customer purchases a large amount of chips (e.g., between $5,000.00 and any sum less than $15,000.00) with currency at a table, engages in minimal gaming, and then goes to the cage and redeems the chips for a casino cheque.

(i) A customer draws casino markers (e.g., between $5,000.00 and $15,000.00) which he uses to purchase chips, engages in minimal or no gaming activity, and then pays off the markers in currency and subsequently redeems the chips for a casino cheque.

(j) While reviewing a casino's computerized player rating records, an employee determines that a customer frequently purchases chips with currency (e.g., between $5,000.00 and any sum less than $15,000.00), engages in minimal gaming and walks away with the chips.

(k) A customer inserts currency into a slot machine bill validator, accumulates credit with minimal or no gaming activity, and then cashes out the tokens or credits at the cage (or slot booth) for large denomination bills or a casino cheque in excess of $2,000.00.

(l) A customer deposits currency (e.g., in the sum of $15,000.00 or more) into a front money/safekeeping account or a race and sports book account, engages in minimal gaming, and later withdraws the funds in the form of currency.

(m) A customer furnishes an identification document, which the casino believes is false or altered (e.g., address changed, photograph substituted, etc.) in connection with the opening of a deposit or credit account.

(n) A customer attempts to exchange several different monetary instruments (i.e., money orders, travelers cheques, personal cheques or business cheques) for a casino cheque and is drawn for the sum of $15,000.00 or more.
(o) A customer who seeks to wire funds, from other than gaming proceeds, to financial institutions within several different jurisdictions.

(p) A customer appears to use a front money/safekeeping account primarily as a temporary repository for funds by making frequent deposits into the account and, within a short period of time (e.g., one to two days), requesting wire transfers of all but a token amount to foreign-based bank accounts.

(q) A customer purchases chips with cash (e.g., in excess of $5,000.00), wagers with little chance of loss (e.g., bets both red and black on roulette), then moves to other gaming tables and conducts similar transactions and later goes to the cage to redeem the chips for large denomination currency or a casino cheque for an amount below $15,000.00.

(r) A customer conducts transactions that the casino believes to be the result of some criminal conduct or from an illegal source (e.g., narcotics trafficking).

(s) A customer, whose transactions contain counterfeit notes or forged instruments, or whose cash has an unusual appearance or smell, suggesting it may have been buried, or some other form of unusual/suspicious feature.

(t) A customer who conducts a number of separate transactions in an apparent attempt to avoid any of the requirements of the Financial Transactions Reporting Act, 2000 for example, a number of transactions under $10,000.00, which in total exceeds $15,000.00, to avoid the customer identification requirements.

(u) A customer who purchases large amounts of casino chips (just under $15,000.00), does not gamble and attempts to cash the chips as “casino winnings” for a cheque.

(v) A customer who buys in with large amounts of cash (just under $15,000.00) at tables or machines does not gamble and then cashes out at the cashier’s cage.

(w) A customer who deposits cash, or who transfers via wire, without a clear intention to wager.

The Financial Intelligence Unit realizes that new typologies of money laundering are constantly evolving. Licensed Casino Operators are encouraged to practice and to record any comments which arise relative to the Guidelines and to forward them to the Financial Intelligence Unit so that amendments may be made where applicable pursuant to the Financial Intelligence Unit Act, 2000, as amended.
EXAMPLES OF SANITISED CASES RELATED TO TERRORIST FINANCING

The cases below have been reproduced (with minor modifications) from those provided by the Egmont Group of Financial Intelligence Units (FIUs).

CASE 1: “Donations” support terrorist organization

A terrorist organization collects money in Country A to finance its activities in another country. The collecting period is between November and January each year. The organization collects the funds by visiting businesses within its own community. It is widely known that during this period the business owners are required to “donate” funds to the cause. The use of threat of violence is a means of reinforcing their demands. The majority of businesses donating funds have a large cash volume. All the money is handed over to the collectors in cash. There is no record kept by either the giver or the receiver. Intimidation prevents anyone in the community from assisting the police, and the lack of documentation precludes any form of audit trail. It is estimated that the organization collects between USD $650,000 and USD $870,000 per year. The money is moved out of the country by the use of human couriers.

CASE 2: Smuggling supports terrorist organization

A terrorist organization is involved in smuggling cigarettes, alcohol and petrol for the benefit of the organization and the individuals associated with it. The goods are purchased legally in Europe, Africa or the Far East and then transported to Country B. The cost of the contraband is significantly lower than it is in Country B due to the different tax and excise duties. This difference in tax duties provides the profit margin. The terrorist organization uses trusted persons and limits the number of persons involved in the operation. There is also evidence to point to substantial co-operation between the terrorist organization and traditional organized crime.

The methods that are currently being used to launder these proceeds involve the transport of the funds by couriers to another jurisdiction. The money typically enters the banking system by the use of front companies or shell companies. The group has also created specialized bureau de change, that exist solely to facilitate the laundering of smuggled proceeds.

The smuggler also sometimes gives the funds to legitimate businesses that are not associated with the smuggling operation. The funds enter the banking system as part of a company’s normal receipts. Monies are passed through various financial institutions and jurisdictions, including locations identified by the FATF as non-cooperative countries and territories (NCCTs).
MONEY LAUNDERING SCHEMES UNCOVERED

Account Opening with Drafts

An investigation into part of an international money laundering operation involving the UK revealed a method of laundering which involved the use of drafts from the Mexican exchange bureaux. Cash generated from street sales of drugs in the USA was smuggled across the border into Mexico and placed into exchange bureaux (cambio houses). Drafts, frequently referred to as cambio drafts or cambio cheques, were purchased in sums ranging from $5,000.00 - $500,000.00. These were drawn on Mexican or American banks. The drafts were then used to open accounts in banks in the UK with funds later being transferred to other jurisdictions as desired.

Bank Deposits and International Transfers

An investigation resulting from a disclosure identified an individual involved in the distribution of cocaine in the UK and money laundering on behalf of a drug trafficking syndicate in the United States of America. Money generated from the sale of the drug was deposited into a UK bank with large sums being later withdrawn in cash and transferred to the USA via a bureau de change. Funds were also transferred by bankers draft. The launderer later transferred smaller amounts to avoid triggering the monetary reporting limits in the U.S. Over an eighteen-month period a total of £2,000,000.00 was laundered and invested in property.

An individual involved in the trafficking of controlled drugs laundered the proceeds from the sales by depositing cash into numerous bank and building society accounts held in his own name. Additionally, funds were deposited into accounts held by his wife. Funds were then transferred to Jamaica where the proceeds were used to purchase three properties amongst other assets.

Currency Exchange

Information was received from a financial institution about a non-account holder who had visited on several occasions exchanging cash for foreign currency. He was known to have an account at another branch nearby and this activity was neither explained nor consistent with his account at the other branch.

The subject of the disclosure was found to have previous convictions for drugs offences and an investigation ensued. The subject was arrested for importing cannabis and later convicted.

APPENDIX F
EXAMPLES OF SUSPICIOUS TRANSACTIONS

1. Money Laundering Using Cash Transactions

(a) Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.

(b) Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.

(c) Customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.

(d) Company accounts whose transactions, both deposits and withdrawals, are denominated by cash rather than the forms of debit and credit normally associated with commercial operations (e.g., cheques, Letters of Credit, Bills of Exchange, etc.)

(e) Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments.

(f) Customers who seek to exchange large quantities of low denomination notes for those of a higher denomination.

(g) Frequent exchange of cash into other foreign currencies without exchange control approval.

(h) Branches that have a great deal more cash transactions than usual. (Head Office statistics detect aberrations in cash transactions.)

(i) Customers whose deposits contain counterfeit notes or forged instruments.

(j) Customers transferring large sums of money to or from overseas jurisdictions with instructions for payment in cash.

(k) Large cash deposits using night safe facilities, thereby avoiding direct contact with licensed financial institution staff.
2. **Money Laundering Using Licensed Financial Institution Accounts**

(a) Customers who wish to maintain a number of trustee or clients accounts which do not appear consistent with the type of business, including transactions which involve nominee names.

(b) Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.

(c) Any individual or company whose account shows virtually no normal personal banking or business related activities, but it is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g., a substantial increase in turnover on an account).

(d) Reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the financial institution to verify.

(e) Customers who appear to have accounts with several financial institutions within the same locality, especially when the institution is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.

(f) Matching of payments out with credits paid in by cash on the same or previous day.

(g) Paying in large third party cheques endorsed in favour of the customer.

(h) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from overseas or an offshore account.

(i) Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.

(j) Greater use of safe deposit facilities. Increased activity by individuals. The use of sealed packets deposited and withdrawn.

(k) Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client companies and trust accounts.

(l) Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.

(m) Large number of individuals making payments into the same account without an adequate explanation.

3. **Money Laundering Using Investment Related Transactions**

(a) Purchasing of securities to be held by the financial institution in safe custody, where this does not appear appropriate given the customer’s apparent standing.

(b) Back-to-back deposit/loan transactions with subsidiaries of, or affiliates of, overseas financial institutions in known drug trafficking areas.
(c) Requests by customers for investment management services (either foreign currency or securities) where the source of the funds is unclear or not consistent with the customer’s apparent standing.

(d) Larger or unusual settlements of securities in cash form.

(e) Buying and selling of a security with no discernible purpose or in circumstances, which appear unusual.

4. **Money Laundering by International Activity**

(a) Customer introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent.

(b) Use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer’s usual business.

(c) Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from countries which are commonly associated with the production, processing or marketing of drugs and proscribed terrorist organizations.

(d) Building up of large balances, not consistent with the known turnover of the customer’s business, and subsequent transfer to account(s) held overseas.

(e) Unexplained electronic fund transfers by customers on an in-and-out basis or without passing through an account.

(f) Frequent requests for traveler’s cheques, foreign currency drafts or other negotiable instruments to be issued.

(g) Frequent paying in of traveler’s cheques or foreign currency drafts, particularly if originating from overseas.

5. **Money Laundering by Secured and Unsecured Lending**

(a) Customers who repay problem loans unexpectedly.

(b) Request to borrow against assets held by the financial institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer’s standing.

(c) Request by a customer for a financial institution to provide or arrange finance where the source of the customer’s financial contribution to a deal is unclear, particularly where property is involved.

6. **Money Laundering Involving Financial Institution Employees and Agents**

(a) Changes in employee characteristics (e.g., lavish lifestyles or avoiding taking holidays).

(b) Changes in employee or agent performance (e.g., the salesman selling products for cash has a remarkable or unexpected increase in performance).
(c) Any dealing with an agent where the identity of the ultimate beneficiary or counterparty is undisclosed, contrary to normal procedure for the type of business concerned.

7. Sales and Dealing Staff

(a) New Business

Although long-standing customers may be laundering money through an investment business, it is more likely to be a new customer who may use one or more accounts for a short period only and may use false names and fictitious companies. Investment may be direct with a local institution or indirect via an intermediary who “doesn’t ask too many awkward questions”, especially (but not only) in a jurisdiction where money laundering is not legislated against or where the rules are not rigorously enforced.

The following situations will usually give rise to the need for additional enquiries:

(a) A personal client for whom verification of identity proves unusually difficult and who is reluctant to provide details.

(b) A corporate/trust client where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation.

(c) A client with no discernible reason for using the firm’s service; e.g., clients with distant addresses who could find the same service nearer their home base, or clients whose requirements are not in the normal pattern of the firm’s business which could be more easily serviced elsewhere.

(d) An investor introduced by an overseas bank, affiliate or other investor both of which are based in countries where production of drugs or drug trafficking may be prevalent.

(e) Any transaction in which the counterparty to the transaction is unknown.

(b) Intermediaries

There are many clearly legitimate reasons for a client’s use of an intermediary. However, the use of intermediaries does introduce further parties into the transaction thus increasing opacity and, depending on the designation of the account, preserving anonymity. Likewise there are a number of legitimate reasons for dealing via intermediaries. However, this is also a useful tactic, which may be used by the money launderer to delay, obscure or avoid detection.

Any apparently unnecessary use of an intermediary in the transaction should give rise to further enquiry.

(c) Dealing Patterns and Abnormal Transactions

The aim of the money launderer is to introduce as many layers as possible. This means that the money will pass through a number of sources and through a number of different persons or entities. Long-standing and apparently legitimate customer
accounts may be used to launder money innocently, as a favor, or due to the exercise of undue pressure.

Examples of unusual dealing patterns and abnormal transactions may be as follows:

(i) **Dealing Patterns**

- a large number of security transactions across a number of jurisdictions.
- transactions not in keeping with the investor’s normal activity, the financial markets in which the investor is active and the business which the investor operates.
- buying and selling of a security with no discernible purpose or in circumstances, which appear unusual; e.g., churning at the client’s request.
- low grade securities purchased in an overseas jurisdiction, sold locally and high-grade securities purchased with the proceeds.
- bearer securities held outside a recognized custodial system.

(ii) **Abnormal Transactions**

- a number of transactions by the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, the proceeds being credited to an account different from the original account.
- any transaction in which the nature, size or frequency appears unusual; e.g., early termination of packaged products at a loss due to front end loading, or early cancellation, especially where cash had been tendered and/or the refund cheque is to a third party.
- transfer of investments to apparently unrelated third parties.
- transactions not in keeping with normal practice in the market to which they relate; e.g., with reference to market size and frequency, or at off-market prices.
- other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or other destinations or beneficiaries.

8 **Settlements**

(a) **Payment**

Money launderers will often have substantial amounts of cash to dispose of and will use a variety of sources. Cash settlements through an independent financial advisor or broker may not in itself be suspicious; however, large or unusual settlements of securities, deals in cash and settlements in cash to a large securities house will usually provide cause for further enquiry. Examples of unusual payment settlements may be as follows:
• a number of transactions by the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction;
• large transaction settlement by cash;
• payment by way of cheque or money transfer where there is a variation between the account holder/signatory and the customer.

(b) Registration and Delivery
Settlement by registration of securities in the name of an unverified third party should always prompt further enquiry.

Bearer securities, held outside a recognized custodial system, are an extremely portable and anonymous instrument, which may serve the purposes of the money launderer well. Their presentation in settlement or as collateral should, therefore, always prompt further enquiry as should the following:

• settlement to be made by way of bearer securities from outside a recognized clearing system;
• allotment letters for new issues in the name of persons other than the client.

(c) Disposition
As previously stated, the aim of money launderers is to take “dirty” cash and to turn it into “clean” spendable money or use it to pay for further shipments of drugs, etc. Many of those at the root of the underlying crime will be seeking to remove the money from the jurisdiction in which the cash has been received, with a view to its being received by those criminal elements from whom it is ultimately destined in a manner, which cannot easily be traced. The following situations should, therefore, give rise to further enquiries:

• payment to a third party without any apparent connection with the investor;
• settlement either by registration or delivery of securities to be made to an unverified third party;
• abnormal settlement instructions, including payment to apparently unconnected parties.

9. Potentially Suspicious Circumstances – Trust Companies

The following are examples of potentially suspicious circumstances, which may give rise to a suspicion of money laundering in the context of Trust Companies:

Suspicous Circumstances Relating to the Customer/Client’s Behavior:

(a) the establishment of companies or trusts which have no obvious commercial purpose;
(b) clients/customers who appear uninterested in legitimate tax avoidance schemes;
(c) sales invoice totals exceeding the known value of goods;
(d) the client/customer makes unusually large cash payments in relation to business activities which would normally be paid by cheques, bankers drafts, etc;
(e) the customer/client pays either over the odds or sells at undervaluation;
(f) customer/clients have a myriad of bank accounts and pay amounts of cash into all those accounts which, in total, amount to a large overall sum;
(g) customers/clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
(h) the payment into bank accounts of large third party cheques endorsed in favour of the client/customer.

**Potentially Suspicious Secrecy may involve the following:**
(a) the excessive or unnecessary use of nominees;
(b) the unnecessary granting of wide ranging Powers of Attorney;
(c) the utilization of a client account rather than the payment of things directly.
(d) the performance of “execution only” transactions;
(e) an unwillingness to disclose the sources of funds;
(f) the use of a mailing address for non-residents;
(g) the tardiness and/or unwillingness to disclose the identity of the ultimate beneficial owners or beneficiaries.

**Suspicious Circumstances in Groups of Companies and/or Trusts:**
(a) companies which continually make substantial losses;
(b) complex group structures without a cause;
(c) subsidiaries which have no apparent purpose;
(d) a frequent turnover in shareholders, directors or trustees;
(e) uneconomic group structures for tax purposes;
(f) the use of bank accounts in several currencies for no apparent reason;
(g) the existence of unexplained transfers of large sums of money through several bank accounts.

It should be noted that none of these factors on their own necessarily mean that a customer/client or any third party is involved in any money laundering. However, in most circumstances a combination of some of the above factors should arouse suspicions. In any event, what does or does not give rise to a suspicion will depend on the particular circumstances.
The Financial Intelligence Unit realizes that new typologies of money laundering are constantly evolving. Banks and Trust Companies are encouraged to practice and to record any comments which arise relative to the Guidelines and to forward them to the Financial Intelligence Unit so that amendments may be made where applicable pursuant to the Financial Intelligence Unit Act, 2000, as amended.
NEW TYPOLOGIES BASED UPON SUB-SECTOR

The FIU has noticed that a trend has been developing relative to email and telephone scams that are consequently affecting many financial institutions within the jurisdiction. The Unit hereby advises all financial institutions and the general public that before any financial transaction is conducted online, pursuant to instructions given via telephone, or otherwise, that they are aware of the nature, manner and source of the proposed transaction. It is recommended that the true identity of the sender or caller be verified. To this end the verification of the sender or caller’s true identity can be achieved by using the verification policies and procedures currently in place by financial institutions. As such we are advising financial institutions to review its policies and procedures with a view of ensuring that stringent mechanisms are in place to prevent the ability of fraudsters to successfully bypass the institution’s policies and procedure. To achieve this objective will require financial institutions to revise and enhance its current due diligence policies and procedure. Persons are further advised that before acting on any proposed transaction it should be fully investigated and a determination made by relevant qualified personnel within the financial institution, as to the authenticity of the transaction request.

Banking

Case # 1 (FIU Bahamas)

Cindy, a business person, opened an investment account with a non-traditional financial institution with funds totaling $600,000.00. The source of the funds was said to be from her numerous businesses. As time went by the non-traditional financial institution noticed that the funds were not being used for any investments. There were no instructions on file as to what to invest in or to purchase. Cindy wanted to place more funds in the account, but the request was denied, due to the annual limit being met. Cindy then tried to open another account with the institution, however, because of the suspicious nature of her actions, the institution decided to report the matter to the FIU. It was later discovered that, the institution was not the only one which had reported Cindy for her actions. It was also discovered that she was known to be involved in the illegal gambling racket. Consequently, the FIU decided to pass the information on to the police department for further investigation.

Indicators: Account not used for its intended purpose; large amount of unused funds sitting in account; institution refuses to accept additional deposits based on suspicion; unsuccessful attempt to open second account at same institution.

Case # 2 (FIU Bahamas)

On 15th July 2011, Mr. Bill visited a local bank, to request a loan for furniture in the amount of $14,000.00. At this point, the subject submitted documents to be reviewed by the Credit Officer. The Credit Officer reviewed the documents and noticed that a large
payment was paid to another financial institution named Gold Trust. The Credit Officer then requested that Mr. Bill provide a credit reference from Gold Trust. Sometime later Mr. Bill provided the credit reference to the Credit Officer. The Credit Officer observed that the “credit reference” was not on Gold Trust’s letterhead. The Credit Officer then contacted the signatory on the reference from Gold Trust to verify the authenticity of the document. The Credit Officer faxed the credit reference to the signatory. Upon receipt of the credit reference, the signatory confirmed that the document was indeed falsified. This resulted in a report being filed with the FIU for analysis and subsequently referred to the police department for investigation.

Indicators: Identification of fraudulent document.

Case # 3 (FIU Bahamas)

Mr. Jay a non resident of the Bahamas came to a financial institution purporting to be a representative of Mr. Tee, who wanted to establish a relationship with the institution. Mr. Jay stated that Mr. Tee could not attend due to a family emergency. Mr. Jay produced a cheque claiming it to be from a reputable organization in the sum of $2,000,000.00 along with a letter of recommendation allegedly from the same reputable organization stating that the cheque was legitimate and requesting that it be deposited in to an account at the financial institution.

The financial institution conducted an internal investigation and discovered that the letter of recommendation and cheque from the reputable organization was false. This matter was then reported to the Financial Intelligence Unit.

It was discovered by the Financial Intelligence Unit that Mr. Jay also approached another financial institution with the same letter along with the cheque of $2,000,000.00. It was also established by the financial institution that the letter and cheque was fraudulent. Further checks conducted by the Financial Intelligence Unit on Mr. Jay, ascertained that Mr. Jay was also implicated in similar offenses in the country where he lived. The police department was informed, and Mr. Jay was arrested on the premises of the institution. Mr. Jay was charged with conspiracy to commit fraud by false pretence, uttering a forged document and attempted fraud by false pretences.

Indicators:

- Unusual- Underlying Business action (Cross border travel to undertake simple transaction);
- Identification of False Document.

Case # 3 (FIU Bahamas)

The police department approached a financial institution in order to freeze an account of Mr. Peel. The financial institution received information that Mr. Peel was allegedly involved in fraud by advertising the import/sale of used cars in newspapers, leading victims to deposit funds to Mr. Peel’s account, which was withdrawn the same day as it
was deposited. The clients who did as the advert stated never received the vehicles, nor their monies back. The financial institution reported the matter to the Financial Intelligence Unit.

On analysis of the account it was discovered that the account was a Savings account and not a business account. The purported funds to be deposited on the account were stated as “Salary”. The monthly activity on the account was well over the anticipated monthly figure on the account opening documents, especially in the months that the victims deposited funds to the account.

Mr. Peel was arrested and charged with stealing by reason of service. A search warrant was issued to search Mr. Peel’s home where withdrawal slips were discovered that corresponded to the dates that persons deposited funds on the account.

Indicators:
- Police enquiries;
- Not in keeping with stated monthly activities.

Case # 4 (FIU Bahamas)

A financial Institution conducted its routine due diligence on a client who had a business account at the institution. The business was in reference to the construction trade. It was discovered that the company’s account was engage in forex trading (financial market for trading currencies) and not in construction as declared in the account opening documents. It was also discovered that all of the deposits were below the $10,000.00 threshold. The financial institution contacted their client, Ms. Key, to clarify this change in business activity, but Ms. Key never replied to the institution. The institution decided to close out the account and report the matter to the Financial Intelligence Unit.

The Financial Intelligence Unit in its search discovered that Ms. Key a former trader on a foreign stock exchange was found guilty of failing to disclose various offenses including one that was subject to statutory disqualification, which resulted in a penalty of censure and a two year ban from trading in his country. It was also discovered that a foreign investigation body had an interest in Ms. Key. Consequently, the Financial Intelligence Unit decided to pass the matter on to the police department for investigation.

Indicators:
- Change of account behavior without explanation;
- Identification of False Document.

Case # 5 (FIU Bahamas)

Ms. Gold approached a financial institution with documents stating to be the recipient of $5,000,000.00 inheritance from a foreign dignitary. She inquired as to the steps she would have to take in order to have the funds wire transferred to her account at the institution. The documents in Ms. Gold possession included a certificate of deposit, death certificate and an affidavit stating that the next of kin would receive the monies belonging to the
foreign dignitary in care of his wife. Upon review by the institution, it was determined that all the documents presented was falsified.

It was discovered by the financial institution that similar scams were being perpetrated on individuals and in some cases the name provided for the foreign dignitary was the same. It was also discovered by the financial institution that Ms. Gold had wired transferred $1,000.00 of her money to the attorney of the foreign dignitary’s wife to assist in carrying out the transfer of funds. When the financial institution inquired on her connection to the foreign dignitary’s wife, Ms. Gold admitted that they became close friends on the Internet. The financial institution reported the matter to the Financial Intelligence Unit, who in turn reported the matter to the police department.

Indicators:

- Internet warning on similar scam;
- Identification of False Documents.

Case # 6 (FIU Bahamas)

On July 15, 2011, Appleton Bank and Trust received an e-mail request from their client Mrs. Jane Keanton to wire funds out of her account. The bank did not find this request to be unusual because Mrs. Keanton was known to make similar requests in the past. The person purporting to be Mrs. Keanton called the bank several times to confirm that the bank received the e-mailed instructions. The bank, before it wired the funds verified the signature of Mrs. Keanton with the signature they had on file and both signatures appeared to be a perfect match. Two weeks later, after additional requests were made for funds to be wired out of the account, an employee of the bank noticed that the known and filed e-mail address of Mrs. Keanton was slightly changed from janekeanton@bmail.com to janekaenton@bmail.com. The bank upon discovering the discrepancies, contacted Mrs. Keanton, who informed bank officials that she did not instruct the bank to transact such business on her behalf. Mrs. Keanton at this time advised the bank that she had recently changed her e-mail address as there was an attempted fraud perpetrated on another one of her accounts.

The bank later reported this matter to the Financial Intelligence Unit and advised that the bank was never informed by its client about the attempted fraud against one of her other account. The bank further reported that the person purporting to be Mrs. Keanton was still awaiting another wire transfer after the bank’s discovery of the fraud. The FIU subsequently reported this matter to the police department for investigation.

Indicators:

- Indication of an e-mail fraud scam.

Case # 7(FIU Bahamas)

Due to an internal investigation conducted by Silverdust Bank & Trust, it was discovered that a client (Mr. Jim Smith), could be the victim of a scam. Jim Smith over an eight month (8) period sent numerous money transfers to high risk countries known fraudulent scams. The bank reported that Mr. Smith informed the bank that he was expecting $1.5
million dollars and wished to inquire about the process of having the funds wired to his account.

The bank further stated that Mr. Smith claimed that he had been in communication with a lady on the internet, whom he refers to as his girlfriend. The bank stated that she claimed to be a lawyer in an Eastern European country. Mr. Smith over time has sent some $32,000.00 to this purported lawyer and over $2,000.00 dollars in the name of a number of other persons domiciled in high risk countries known for their fraudulent scams.

The bank also stated that it is highly unlikely, based on his occupation, that Mr. Smith was financially capable of sending this amount of funds from his personal finances. The bank reported this matter to the FIU, because it is believed that Mr. Smith is involved in money laundering either as an active participant, or is a victim to fraud.

Indicators:

- Indication of an e-mail fraud scam;
- Large funds being sent to countries known for fraudulent scams with no legitimate reason;
- Account activity not in keeping with KYC.

Case # 8 (FIU Bahamas)

Peter, James & John Law firm was contacted via e-mail by a female purporting to be Mary Jones, who requested legal services in reference to assisting in the collection of a debt owed to her. The law firm in turn requested that Ms. Jones provide more information in regards to the matter, inclusive of Know Your Customer (KYC) information, so that the law firm could best advise her. A few days after the initial e-mail from Ms. Jones, she provided Peter, James & John Law Firm a scanned copy of the debt agreement. The alleged debt was in the amount of $250,000.00. Ms. Jones was then given advice on the matter and what steps needed to be taken to it resolved. Ms. Jones then requested that the law firm serve a demand letter on Ms. Tiffany Rolle (the debtor). Ms. Jones provided the law firm with a signed document, purporting the same to be an engagement agreement between the law firm and herself, but still failed to pay the retainer requested by the law firm. Additionally, Ms. Jones did not provide any (KYC) information, which, along with further e-mails from Ms. Jones referring to the debtor as Ms. Tiffany Johnson instead of Ms. Tiffany Rolle, further raised the law firm’s suspicion.

Sometime later, Ms. Jones was e-mailed by the firm and was requested to again provide all of the necessary documentation, or the firm would have to consider the matter closed.

Three days later the firm received a cheque with a cover letter via Speedy Postal Service purporting to be from Ms. Tiffany Rolle and issued by Community Bank. This was highly suspicious to the firm because they were never properly instructed to act, Ms. Rolle was never contacted by the firm to send any money to them on behalf of Ms. Jones and the cheque appeared to be fraudulent.

Due to the suspicious nature of the matter the firm decided to report the matter to the FIU.
Indicators:

- Identification of false documentation;
- Indication of an e-mail fraud scam;
- Refusal to fill out due diligence requirement.

Case # 9 (FIU Bahamas)

Gombay Bank & Trust was informed by its customers and non-customers alike that they were receiving e-mails from Gombay Bank & Trust requesting that they select an attached link to receive a secure mail statement from the bank. Gombay Bank and Trust informed its customers that it is not the policy of the bank to communicate with a customer or transmit a customer’s information via e-mails.

During the summer months Gombay Bank and Trust received an online request from a customer Mr. Brown to transfer funds to a lady in a country in Africa. The bank conducted the transaction and e-mailed the customer to state that the transaction was completed. At this point Mr. Brown stated that he did not request a transfer. After discussing the matter further with Mr. Brown it was discovered by the bank that Mr. Brown had also received an e-mail supposedly from Gombay Bank & Trust instructing him to open an attachment link to receive a secured mail statement, which he opened. It was also discovered by the bank that this fraud affected more of their online customers than was first thought.

Consequently, the bank initiated a policy to contact all online customers before a request is processed. This matter was reported to the FIU and subsequently reported to the police department for investigation.

Indicators:

- Indication of an e-mail fraud scam;
- Large funds being sent to countries known for fraudulent scams;
- Indication of on-line hacking.

Nigerian Letter Scam (419)

This relates to a fraudulent scheme that now includes fax and e-mail versions of a letter from a supposed official in Nigeria. The official allegedly has a large sum of money (often stated as $20 to $30 million) to transfer out of the country. Due to exchange controls, the official asks for the victim’s help with the transfer. All that is required to earn a hefty reward/commission is to furnish the Nigerian official with your bank account number, and they will handle the rest. What actually happens is that the perpetrator depletes the victim’s account.

In other instances, it is suspected that Bahamians have been duped into sending monies to perpetrators via wire transfers. (FIU Bahamas).
FATF Sanitized Cases

Investment Business

During the course of an investigation made by the FIU in Country X, regarding proceeds from drug trafficking an individual was identified acting as branch manager of a local foreign exchange broker involved in ML activities and, later on, acting as account executive for a broker-dealer who was arranging wire transfers for one of his customers. Accordingly, the FIU informed the broker-dealer of this activity and it submitted an STR with no specific information. Further investigations showed that an account at this broker-dealer was used to send money abroad in the following way:

The broker-dealer received several cheques in local currency, in the name of different persons but all of them endorsed to the same account holder (the sender). Funds were withdrawn immediately (the same day) with a purchase of US$ and a further wire transfer abroad was arranged for one single beneficiary (different from the sender). This money was ultimately used to pay for the purchase of real estate in Country Y.

The outcome of this investigation was the seizure of many assets, including among others, bank accounts and aircraft and the closing of the foreign exchange broker involved.

Indicators: Activity reported by senders to financial institutions is not related in any way to the beneficiary of funds; amounts transferred are not congruent with the purchase of products; FX dealer-broker or bureau de change ordered the transfers abroad (and not the senders); common beneficiaries with other customers using the same operating procedure; and same day withdrawal of funds.

Offence: Money laundering.

Trust Services

Mr. B set up an international structure with on and offshore trust to purchase insurance companies. The insurance companies were actually bought through a trust to hide the personal involvement of B. The assets of these companies were subsequently drained and used for personal benefits. The draining of the assets was concealed by transferring money into accounts in and out of the US via wire transfers. Immediately after the acquisitions, B would transfer millions of dollars of reserve assets to a corporation he set up in the US. The funds were transferred to an offshore bank account in the name of another corporation that he controlled. Once these funds were deposited in the offshore
bank account, B used them to pay his personal expenses. In this way, B laundered about US$225 Million over a period of 9 years.

Insurance:

Numerous motor vehicles owned by a number of companies were insured. As part of the process for setting up the insurance policies various company documents were reviewed by the insurer. The companies had been incorporated during 1994 – 1995 when Mr. X was 24 years old. The registered business activities of the companies set out significant investments that did not correspond to the age and status of Mr. X.

The companies appeared to be linked to other persons related to Mr. X and were incorporated with the same address.

Subsequently, Mr. X refused to provide information on the origin of funds used to acquire the motor vehicles.

Indicators: false or inconsistent declarations; refusal to provide information on source of funds.

Offence: Money Laundering.

Casinos

The money laundering conspiracy involved millions of UK Pounds from organized criminal gangs being laundered by a group of men from West Midlands. The money laundered included profits from a number of activities drug trafficking, multi-million pounds VAT conspiracies in the mobile phone industry, counterfeiting and credit card fraud. The monies were a mixture of Scottish and English notes. The defendants would transfer a large amount of money to a bank account in Dubai, which would then be accessed by their associates. The defendants received the proceeds of crime in the UK and made equivalent amounts of criminal monies available to Dubai. They then utilized the gaming industry to launder the money. Money was placed on deposit at a casino then withdrawn a day or so later. Other sums would be gambled. Thousands of pounds would be passed over the tables in order to disguise the original source of the bank notes. Moneys gambled or exchanged at the casino provided the defendants with an apparent legitimate explanation as to their source.

Indicators: Transfer of funds from/to a foreign casino/bank account; funds withdrawn from account shortly after being deposited; use of intermediaries to make large cash deposits; use of a casino account as a savings account; large amount of cash from unexplained sources.

Offences: Money laundering; VAT Fraud; counterfeiting; credit card fraud; drug smuggling.
Real Estate

A company purchased property by using a notary’s client account. Apart from a considerable number of cheques that were regularly cashed or issued, which at first sight were linked to the notary’s professional activities, there were also various transfers from the company to his account.

By using the company and the notary’s client account money was laundered by investing in real estate in Country X and the links between the individual and the company were concealed in order to avoid suspicions.

Police sources revealed that the sole shareholder of the company was a known drug trafficker.

Indicators: Intermediary account; purchase of real estate; and incoming wire transfers.

Offence: Suspected trafficking in narcotics.

Non-Profit Organizations/Charities

A charity was suspected of raising and disbursing financial resources for a terrorist organization based in another country. Over a period of five years, the charity organized a “substantial” number of electronic funds transfers to overseas-based persons and entities, including a charity that was thought to be operating as a front for a terrorist group. During the same five year period, large sums of cash were deposited into, and multiple credits made to, the charity’s accounts. The source of funds was unknown as was the identity of the remitter for the credits. Cash deposits into the accounts were immediately followed by the purchase of bank drafts or for the transfer of funds overseas.
APPENDIX H

SUSPICIOUS TRANSACTION REPORT

Completed forms should be forwarded by hand, facsimile or courier to 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, Facsimile No.: (242) 322-5551

For Official Use Only

FIU Reference Number: .................................................................

To: Financial Intelligence Unit – Fax No.: (242) 322-5551

Date: ____________________________ No. of Pages: ________________

N.B: Persons who report suspicious transactions are required, pursuant to provisions of the Financial
Transactions Reporting Act, 2000 and the Anti-Terrorism Act 2004, to provide the Financial Intelligence Unit
with the following information:

[A] Disclosing Institution

Disclosure Type: Proceeds of Crime ☐ Report No.: .................................................................
Drug Trafficking ☐ Type of Transaction: .................................................................
Terrorism Finance ☐ .................................................................
Other ☐ .................................................................

Name of Disclosing Institution: .................................................................
Full Address: .................................................................................................
Sort Code: .................................................................................................
Name of Person Handling Transaction: .................................................................
Name of Money Laundering Reporting Officer/Contact Person: .................................................................
Direct Telephone No: ...............................................................................................................
Fax: .........................................................................................................................
E-mail Address: .............................................................................................................

[B] Subject(s) of Disclosure – Individual

Full Name (Individual): .................................................................................................
Date and Place of Birth: .................................................................................................
Occupation: ....................................................................................................................
Full Address: ....................................................................................................................

FIU’S GUIDELINES
FOR FINANCIAL INSTITUTIONS - ............ 2013

118
[C] Subject(s) of Disclosure – Company

Company Name: ..........................................................
Type of Business: ..........................................................
Full Address: ............................................................

Telephone No.: ......................................................... Fax No.: ..........................................................

E-mail Address: ..........................................................
Identification Documents (e.g., certificate of incorporation, memorandum and articles of association, etc. if available): .......

[D] Beneficial Owner(s)

(of the assets being the subject(s) of disclosure – if different from the subject(s) of disclosure above)

Full Name: ................................................................
Date and Place of Birth (Individual): ..........................................................

Type of Business/Occupation: ..........................................................
Full Address: ............................................................

Telephone No. (Work): ................................................. Telephone No. (Home): ..............................................

Fax: ......................................................................... E-mail Address: ..........................................................

[E] Authorized Signatories

Information on authorised signatories and/or persons with power of attorney.
(List further persons in an annex in the same manner as required below)

Full Name (Individual): ................................................................
Date and Place of Birth (Individual): ..........................................................
Occupation: ...........................................................................................................

Full Address: ........................................................................................................
.........................................................................................................................
.........................................................................................................................
.........................................................................................................................
.........................................................................................................................

Telephone No. (Work): ................................ Telephone No. (Home): .........................
Fax: ................................................................. E-mail Address: ..............................

[F] Intermediaries

Full Name (Individual): .........................................................................................

Occupation: ............................................................................................................
.........................................................................................................................
.........................................................................................................................

Full Address: ........................................................................................................
.........................................................................................................................
.........................................................................................................................

Telephone No. (Work): ................................ Telephone No. (Home): .........................
Fax: ................................................................. E-mail Address: ..............................

[G] Account Information/Activity

Type of Account: (e.g., individual/joint, trust, loan, etc.): ........................................

Account number: ...................................................................................................

Date Opened: .........................................................................................................

Date Closed: .........................................................................................................

Assets Held: .......................................................................................................... 

Jurisdiction Where Assets Are Held: ......................................................................

Other Accounts Held by any of the Parties Involved: ................................................

REASONS FOR SUSPICION

<table>
<thead>
<tr>
<th>Details of Sums Arousing Suspicion Indicating Debit or Credit Source and Currency Used</th>
<th>Amount</th>
<th>Debit or Credit</th>
<th>Date</th>
<th>Source</th>
<th>Currency</th>
</tr>
</thead>
</table>

Please describe the details of the transaction(s) and the activity that promoted the report, giving reason for your suspicion and any steps that have already been taken (e.g., own investigations). Include information on any third party(s) involved (e.g., payee, payer, deliverer of cheques, stocks, guarantee beneficiary, guarantee surety, third party security creditors). Please add continuation sheets as necessary.
You are asked to assist with completing the attached statistical analysis, which will help us to give you feedback – Thank you!
## STATISTICAL INFORMATION

<table>
<thead>
<tr>
<th>Nature of Institution</th>
<th>Please tick</th>
<th>Grounds for Disclosure?</th>
<th>Please tick</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank</td>
<td></td>
<td>Media / Publicity</td>
<td></td>
</tr>
<tr>
<td>Fund Manager</td>
<td></td>
<td>Internet Research</td>
<td></td>
</tr>
<tr>
<td>Bureaux Des Changes</td>
<td></td>
<td>Group Information</td>
<td></td>
</tr>
<tr>
<td>Stockbroker</td>
<td></td>
<td>3rd Party Information</td>
<td></td>
</tr>
<tr>
<td>Financial Advisor</td>
<td></td>
<td>Service of Production, Charging or Monitoring Order</td>
<td></td>
</tr>
<tr>
<td>Insurance Company</td>
<td></td>
<td>Police enquiry</td>
<td></td>
</tr>
<tr>
<td>Trust Company</td>
<td></td>
<td>Account Activity Not in Keeping with KYC</td>
<td></td>
</tr>
<tr>
<td>Corporate Service Provider</td>
<td></td>
<td>Evidence of Forged Documentation</td>
<td></td>
</tr>
<tr>
<td>Lawyer</td>
<td></td>
<td>Cash Transactions</td>
<td></td>
</tr>
<tr>
<td>Accountant</td>
<td></td>
<td>Transitory Accounts – Immediate Layering</td>
<td></td>
</tr>
<tr>
<td>Casino</td>
<td></td>
<td>High Risk Jurisdictions</td>
<td></td>
</tr>
<tr>
<td>Real Estate Agent/Broker</td>
<td></td>
<td>Purchase and Surrender of Insurance Policy</td>
<td></td>
</tr>
<tr>
<td>Credit Union</td>
<td></td>
<td>Unusual Forex Transactions</td>
<td></td>
</tr>
<tr>
<td>Alternative Remittance</td>
<td></td>
<td>Repeat disclosures</td>
<td></td>
</tr>
<tr>
<td>Local Regulator</td>
<td></td>
<td>Failure to comply with due diligence checks</td>
<td></td>
</tr>
<tr>
<td>Other Regulator</td>
<td></td>
<td>Other (specify)</td>
<td></td>
</tr>
<tr>
<td>Other (specify)</td>
<td></td>
<td>Criminality Suspected</td>
<td></td>
</tr>
<tr>
<td>Customer/Transaction Type</td>
<td></td>
<td>Drugs</td>
<td></td>
</tr>
<tr>
<td>Involving at least one intermediary</td>
<td></td>
<td>Terrorism</td>
<td></td>
</tr>
<tr>
<td>Long Standing Customer</td>
<td></td>
<td>Fraud</td>
<td></td>
</tr>
<tr>
<td>New Customer</td>
<td></td>
<td>Revenue Fraud</td>
<td></td>
</tr>
<tr>
<td>Electronic Banking</td>
<td></td>
<td>Insider Dealing</td>
<td></td>
</tr>
<tr>
<td>EURO Transaction</td>
<td></td>
<td>Corruption</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trafficking in Persons</td>
<td></td>
</tr>
<tr>
<td>What currency was involved?</td>
<td></td>
<td>Weapons and Ammunition Trafficking</td>
<td></td>
</tr>
<tr>
<td>GBP</td>
<td></td>
<td>Ponzy Schemes and Lotteries</td>
<td></td>
</tr>
<tr>
<td>USD</td>
<td></td>
<td>Possession, Theft and/or Trafficking in Stolen Gold or other precious metals</td>
<td></td>
</tr>
<tr>
<td>EUR</td>
<td></td>
<td>Financing of Proliferation of Weapons of Mass Destruction</td>
<td></td>
</tr>
<tr>
<td>CAD</td>
<td></td>
<td>United Nations Security Council Resolutions</td>
<td></td>
</tr>
<tr>
<td>JPY</td>
<td></td>
<td>Illegal gambling</td>
<td></td>
</tr>
<tr>
<td>MXN</td>
<td></td>
<td>Cyber crimes</td>
<td></td>
</tr>
<tr>
<td>BRL</td>
<td></td>
<td>Regulatory Matters</td>
<td></td>
</tr>
<tr>
<td>SEK</td>
<td></td>
<td>Tax matters</td>
<td></td>
</tr>
<tr>
<td>CHF</td>
<td></td>
<td>Unknown / undetermined</td>
<td></td>
</tr>
<tr>
<td>BSD</td>
<td></td>
<td>Other</td>
<td></td>
</tr>
</tbody>
</table>

Completed forms should be forwarded to the Financial Intelligence Unit, 3rd Floor Norfolk House, Frederick Street, P. O. Box SB-50086, Nassau, The Bahamas,
Your Ref: 
Our Ref: 
Date: 

...20XX

Name of Financial Institution  
Street Address  
Nassau, The Bahamas  

Attention: Mr./Mrs./Ms..................  
Money Laundering Reporting Officer  

Dear Sir:  

Re: Suspicious Transaction Report in Respect to.......  

The Financial Intelligence Unit acknowledges receipt of your report dated _________ 200X, in respect to the subject at above captioned.  

I wish to advise that our analysis of the report has begun and I shall revert to you at a later date with respect to our findings.  

Yours sincerely,  

Reuben S. Smith, QPM, RVM  
Director  
Financial Intelligence Unit
Financial Intelligence Unit
3rd Floor Norfolk House, Frederick Street,
P. O. Box SB-50086
Nassau, The Bahamas
Tel. Nos.: (242) 356-9808 or (242) 356-6327
Fax No: (242) 322-5551

Name of Financial Institution
Street Address
Nassau, The Bahamas

Attention: Mr./Mrs./Ms. ......................
Money Laundering Reporting Officer

Dear Sir:

Re: Suspicious Transaction Report in Respect to…….

The Financial Intelligence Unit acknowledges receipt of your report dated ____________ 200X, with respect to the captioned matter.

Pursuant to Section 4(2)(d) of the Financial Intelligence Unit Act 2000, the Financial Intelligence Unit requests the production of information, excluding information subject to legal professional privilege, in possession of ................................., in respect.................................

Copies of the following documents will suffice:

a) Account opening documents, including documents which were obtained by your institution during its due diligence exercise, in respect to account number(s) .........................

b) Photo identification of signatories and/or beneficial owner(s).

c) Statement of accounts from inception to present.

d) Incoming and outgoing wire transfers of funds.
e) Correspondences to, from or on behalf of account holders, signatories and/or beneficial owner(s).

f) Memoranda relating to the said accounts.

Yours sincerely,

Reuben S. Smith, QPM, RVM
Director
Financial Intelligence Unit
SOURCES UTILIZED IN PREPARING THE 2013 GUIDELINES

1. Australian Transactions Reports and Analysis Centre (AUSTRAC), Australia.


5. Bahamian Financial Services Legislation by Bahamas Financial Services Board.

6. Telephone Interview with Mr. Charles Turner, Comptroller, Bahamas Customs Department, August 2013.

7. Telephone Interview with Mr. Gerard Horton, Manager, Exchange Control Department, Central Bank of The Bahamas, August 2013.


10. Nassau Public Library, Nassau, Bahamas.


15. *Cases/Typologies* by Egmont Group of FIUs.


17. Serious Organized Crime Agency (SOCA), U.K.


19. *Weapons of Mass Destruction* by Dr. Laura Reed, Hampshire College, Massachusetts, USA.


21. *Migration Fundamentals Trafficking, Smuggling and Human Rights* by Jacqueline Bhabha, Harvard University, Cambridge, Massachusetts, USA.


23. *Illicit Firearms as a Threat to Global Security* by United Nations Office on Drugs and Crime, Vienna, Austria.

24.1. **People Smuggling** by Wikepedia.


27. *Cyber Crime and Bangladesh Perspective* by A.R.M. Borhanuddin (Raihan) Department of Law Dhaka University Ramna, Bangladesh.


31. *FATCA: A New Disclosure and Withholding Regime*, Deloitte Tax LLP, USA.
## GLOSSARY OF TERMS AND ABBREVIATIONS

<table>
<thead>
<tr>
<th>TERM / ABBREVIATION</th>
<th>MEANING</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML/CFT</td>
<td>Anti-Money Laundering and Combating the Financing of Terrorism.</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence.</td>
</tr>
<tr>
<td>Central Bank</td>
<td>Central Bank of The Bahamas.</td>
</tr>
<tr>
<td>DNFBPs</td>
<td>Designated Non-Financial Business and Professions.</td>
</tr>
<tr>
<td>EDD</td>
<td>Extended Due Diligence.</td>
</tr>
<tr>
<td>FIU</td>
<td>Financial Intelligence Unit.</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer.</td>
</tr>
<tr>
<td>MLRO</td>
<td>Money Laundering Reporting Officer.</td>
</tr>
<tr>
<td>NPO</td>
<td>Non-Profit Organization.</td>
</tr>
<tr>
<td>PAN</td>
<td>Primary Account Number.</td>
</tr>
<tr>
<td>PEP</td>
<td>Politically Exposed Person, i.e. a person in The Bahamas or in a foreign country entrusted with public functions, their family members or close associates.</td>
</tr>
<tr>
<td>STR</td>
<td>Suspicious Transactions Report.</td>
</tr>
<tr>
<td>POCA</td>
<td>Proceeds of Crime Act, 2000, as amended.</td>
</tr>
<tr>
<td>ATA</td>
<td>Anti-Terrorism Act, 2004, as amended.</td>
</tr>
<tr>
<td>WMD</td>
<td>Weapons of Mass Destruction.</td>
</tr>
<tr>
<td>FIUA</td>
<td>Financial Intelligence Unit Act, 2000 as amended.</td>
</tr>
<tr>
<td>FITRR</td>
<td>Financial Intelligence (Transactions Reporting) Regulations, 2001 as amended.</td>
</tr>
<tr>
<td><strong>Criminal Conduct</strong></td>
<td>Drug Trafficking; Bribery and Corruption; Money Laundering; an Offence under the Anti-Terrorism Act, 2004; an Offence subject to trial in the Supreme Court other than a Drug Trafficking Offence; an Offence under the POCA.</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Facility</strong></td>
<td>Any account or arrangement which is 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.</td>
</tr>
<tr>
<td><strong>Facility Holder</strong></td>
<td>A person in whose name the facility is established and includes any person to whom that facility is assigned or who is authorized to conduct transactions through that facility.</td>
</tr>
<tr>
<td><strong>Financial Institution</strong></td>
<td>As defined in Section 3 of the FTRA.</td>
</tr>
<tr>
<td><strong>Occasional Transaction</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Source of Funds</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>Source of Wealth</strong></td>
<td>The means by which a customer acquires his wealth (e.g. through a business or an inheritance).</td>
</tr>
<tr>
<td><strong>Tax Information Exchange Agreements (TIEAs)</strong></td>
<td>Tax Information Exchange Agreements or TIEAs are bilateral agreement by which countries make arrangements to cooperate for the exchange of information in relation to tax matters. Signed agreements enter into force when the necessary internal procedures in the signatory countries have been completed.</td>
</tr>
</tbody>
</table>