SUSPICIOUS TRANSACTIONS GUIDELINES RELATING TO THE PREVENTION OF MONEY LAUNDERING AND THE FINANCING OF TERRORISM

FOR FINANCIAL INSTITUTIONS IN THE COMMONWEALTH OF THE BAHAMAS

Issued 19th March 2007,
by:
THE FINANCIAL INTELLIGENCE UNIT
3rd Floor, Norfolk House
Frederick Street
P.O. Box SB-50086
Nassau, The Bahamas
Tel. No: (242) 356-9808 or (242) 356-6327
Fax No: (242) 322-5551

SUSPICIOUS TRANSACTIONS GUIDELINES FOR FINANCIAL INSTITUTIONS RELATING TO PREVENTION OF MONEY LAUNDERING AND THE FINANCING OF TERRORISM

SCOPE

These Guidelines replace those, which were initially issued by the Financial Intelligence Unit (the "FIU") in July 2001. 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 I**, and is grateful for such assistance.

The Guidelines apply to all financial institutions in The Bahamas, as defined in Section 3 of the Financial Transactions Reporting Act, 2000.

These 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. They are produced to accord with the financial laws and business practices of The Bahamas.

I - EXPLANATORY FOREWORD

1. The Bahamian Parliament approved the ***Financial Intelligence Unit Act, 2000 (the "Act")*** in December 2000. The Act 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, 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) 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.

2. The Financial Intelligence Unit of The Bahamas is empowered by Section 15 of the Financial Intelligence Unit Act, 2000, Chapter 367, 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, and the Anti-Terrorism Act 2004 (No. 25 of 2004) 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.

3. The Proceeds of Crime Act, 2000 repealed the Money Laundering (Proceeds of Crime) Act, 1996 (Act No. 8 of 1996), as well as the Tracing and Forfeiture of Proceeds of Drug Trafficking Act, (Chapter 86). The Proceeds of Crime (Money Laundering) Regulations, 2001 (Statutory Instrument No. 8 of 2001) repealed the Money Laundering (Proceeds of Crime) Regulations, 1996 (Statutory Instrument No. 69 of 1996). The Proceeds of Crime Act, 2000 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) reporting of suspicious transactions.

4. The Anti-Terrorism Act, 2004 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.

II - BACKGROUND

WHAT IS MONEY LAUNDERING?

5. 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. 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.

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

6.1 **I. <u>Placement</u>** 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.

6.2 **II. <u>Layering</u>** 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
- resale of goods/assets.

6.3 **III** **<u>Integration</u>** 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.

7. 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.

8. 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.

9. 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.

10. The Bahamas has seen little evidence of placement taking place. 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 G** attached hereto.

11. 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.

12. **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.

TERRORISM AND THE FINANCING OF TERRORIST ACTIVITY

13. 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.

14. 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.

15. 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.

III - DEFINITION OF FINANCIAL INSTITUTIONS

16. This document contains guidelines which are intended to be illustrative of best industry practice and shall apply to any person or body carrying on or providing financial services in or from within The Bahamas. In this context, the term "financial institution" means any of the following: -

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;
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:
   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.

17. The Courts, in determining if the financial institution has satisfactory internal procedures with the organization, shall have regard to any relevant Guidelines issued by the Financial Intelligent Unit on this issue.

IV - PURPOSE AND STATUS OF THE GUIDELINES

18. The Financial Intelligence Unit, following extensive consultation with local financial services regulators, initially issued comprehensive Guidelines in 2001 various categories of Bahamian licensed financial institutions to assist these institutions in understanding and adapting to the new regulatory environment, which had evolved from legislation, which were implemented in December 2000. These Guidelines covered anti-money laundering policies and procedures as well as requirements for suspicious transactions reporting.

19. During the intervening period, local financial sector regulatory agencies have formulated and issued to their respective constituents sector specific AML/CFT Guidelines covering best practices and minimum for preventing money laundering and terrorism financing but excluding suspicious transactions reporting. The international conventions on terrorism **(see Appendix A)** set out the framework for anti-terrorism legislation to which The Bahamas responded with the enactment of the Anti-Terrorism Act, 2004. Thus, these AML/CFT Guidelines address changes in the AML/CFT statutory regime of The Bahamas, such as the enactment of the Anti-Terrorism Act, 2004 as well as changes in international best practices.

20. Based on the aforementioned developments, the FIU considers the time appropriate to update its Guidelines to encompass matters related to the financing of terrorism, and to re-issue same to the financial services sector, but with a narrower focus on the processes related to Suspicious Transactions Reports (STRs). Accordingly, the revised Guidelines attempt to: -

a) explain the requirements of Bahamian Anti-Money Laundering and Anti-Terrorism Financing Legislation;
b) provide a practical interpretation of the Financial Intelligence (Transactions Reporting) Regulations 2001;
c) provide an indication of good industry practice;
d) provide a basis for implementation of policies and procedures for the handling of suspicious transactions; and
e) explain the process for reporting of Suspicious Transactions to the FIU.

21. Where a financial institution has a primary regulator, that regulator's Guidelines/Guidance should take precedence, save in areas which are within the FIU's mandate and for which the FIU has responsibility.

V - WHAT THE BAHAMIAN LAW REQUIRES

22. The Bahamian law relating to money laundering and terrorism financing is contained in the following legislation: -

- The Proceeds of Crime Act, 2000;
- The Financial Transactions Reporting Act, 2000;
- The Financial Transactions Reporting Regulations, 2000;
- The Financial Intelligence Unit Act, 2000;
- The Financial Intelligence (Transactions Reporting) Regulations, 2001;

- The Anti-Terrorism Act, 2004.

The Proceeds of Crime Act, 2000

23. 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.

23.1 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

24. 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

25. 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

26. 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

27. 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

28. 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.

VI - THE ROLE OF THE MONEY LAUNDERING REPORTING OFFICER

29. The type of person appointed as Money Laundering Reporting Officer 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. Larger organizations may choose to appoint a senior member of their Compliance, Internal Audit or Fraud Departments. In small organizations, it may be appropriate to designate the Chief Executive. 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.

30. 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.

31. 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 a 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.

32. 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.

33. 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

34. 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.

35. 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.

36. 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.

37. 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

38. 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.

39. 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.

40. 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.

41. 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.

42. 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

43. 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.

44. 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

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

46. 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.

47. 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.

48. 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

49. 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.

50. 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

51. 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 and consent to undertake the transaction is required from the FIU.

52. 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.

53. 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.

54. 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.

VII - WHAT IS A SUSPICIOUS TRANSACTION?

55. "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.

56. 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.

57. 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.

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

- any unusual financial activity of the customer in the context of his own usual activities;
- any unusual transaction in the course of some usual financial activity;
- any unusually-linked transaction;
- any unusual employment of an intermediary in the course of some usual transaction or financial activity;
- any unusual method of settlement;

- any unusual or disadvantageous early redemption of an investment product;
- any significant cash transactions;
- any activity, which raises doubts as to the client's true identity.

59. 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.

60. 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.

61. 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.

VIII - REPORTING OF SUSPICION

ALL SUSPICIOUS TRANSACTIONS

62. 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.

63. 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.

64. Reporting of a suspicion of criminal conduct is important as a defence 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.

65. 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*;*
- that the Money Laundering Reporting Officer should be resident in The Bahamas in order to facilitate the expeditious reporting of all suspicious transactions to the Financial Intelligence Unit.

66. Staff should be required to report any suspicion of laundering of the proceeds of crime either directly to their Money Laundering Reporting Officer or, if the financial services business so decides, to their line manager for preliminary investigation in case there are any known facts which may negate the suspicion. Financial services businesses are not expected to perform the role of detectives.

67. 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.

68. 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.

69. 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.

70. 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 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.

71. Local financial legislation imposes a duty on banks and trust companies 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.

72. 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.

73. 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

74. 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, 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

75. Examples of what might constitute suspicious transactions are given in **Appendix F**. 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

76. 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.

76.1 Where a financial institution chooses to out source a function within its organization/group 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.

IX - REPORTING TO THE FINANCIAL INTELLIGENCE UNIT (FIU)

77. 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. The financial institution may also wish to notify its primary regulator as to the identity of the Money laundering Reporting Officer. 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.

78. Where an entity does not provide the financial services outlined in paragraph 16 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

79. If the Money Laundering Reporting Officer decides that a disclosure should be made, a report, preferably in standard form **(see Appendix G)**, 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.

80. 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 H**. 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.

81. 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.

82. 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 report on the account, any further transactions and or actions taken by the FIU and the financial institution.

FEEDBACK FROM THE FIU

83. 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.

84. 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

85. 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. 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.

86. 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

87. 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

88. 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.

89. 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.

X - REPORTING PROCEDURES

90. 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.

91. The use of a standard format in the reporting of disclosures is important and should be followed. The form illustrated in **Appendix G** 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.

92. 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.

93. 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.

94. 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.

95. 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.

96. 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.

97. Financial institutions are reminded that reporting to entities identified in Section 18 of the Financial Transactions Reporting Act, 2000 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.

98 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.

XI - USE OF THE FINANCIAL SYSTEM

99. 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 D** provide examples of the trends outlined above.

XII - SOURCES AND USES OF FUNDS

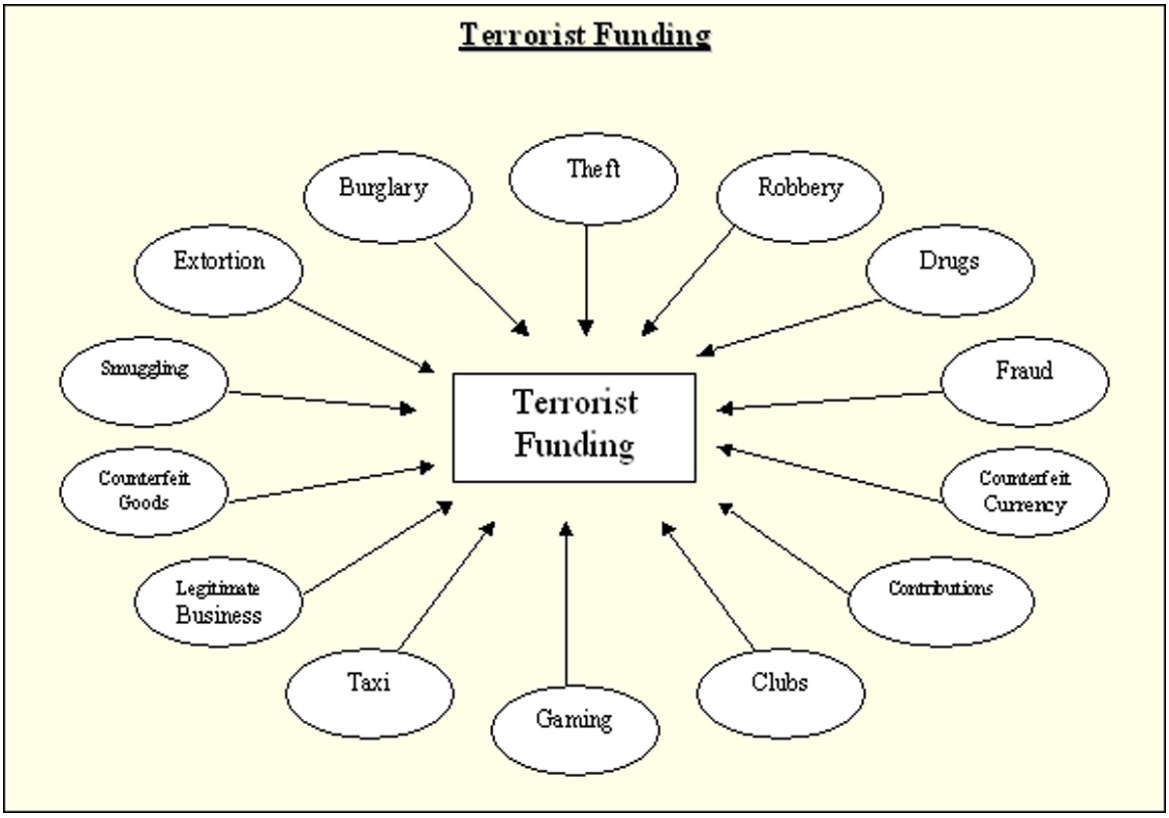
FUNDING SOURCES

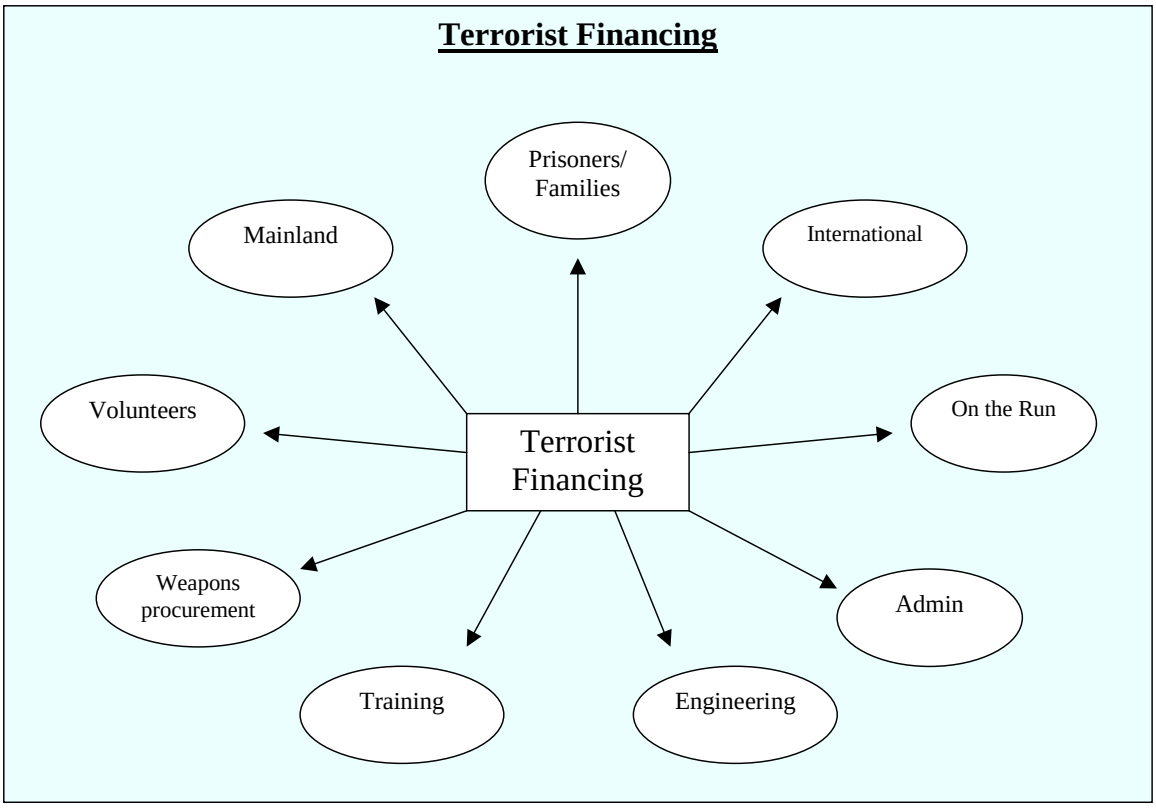
100. As indicated in the diagram immediately below/overleaf, terrorist financing may be derived from legitimate or illegitimate sources. It may be derived from criminal conduct, i.e. counterfeiting, kidnapping, extortion, fraud or drug trafficking. It may also be derived from legitimate income such as membership dues, sale of publications, or income from legitimate business operations belonging to terrorist organizations.

USES OF FUNDS

101. 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.





XIII - BUSINESS-CLIENT RELATIONSHIP

102. 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.

103. 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.

104. 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.

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

XIV - MONEY LAUNDERING AND FINANCING OF TERRORISM OFFENCES, PENALTIES AND DEFENCES

Proceeds of Crime Act, 2000:

Concealing or Dealing with the Proceeds of Criminal Conduct

106. 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.

106.1. **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

107. 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.

107.1 **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.

107.2 **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

108. 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.

108.1 **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.

108.2 **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

109. 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.

109.1 **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.

109.2 **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.

109.3 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, will satisfy the requirement to report suspicious transactions. The Financial Transactions Reporting Act, 2000 and The Financial Intelligence Unit Act, 2000 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:

Suspicion

110. 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, or any offence under the Proceeds of Crime Act, 2000 or an attempt to avoid the enforcement of any provision of the Proceeds of Crime Act, 2000, shall, as soon as practicable after forming that suspicion, make a report to the Financial Intelligence Unit.

110.1 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.

110.2 **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

111. 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. 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. 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.

111.1 **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.

111.2 **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

111.3 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.

111.4 **Penalty**: On summary conviction to imprisonment for a term not exceeding two years.

111.5 **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

112. **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.

112.1 **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

113. **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

114. **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.

114.1 **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

115. **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

116. **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).

Freezing of funds

117. **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

118. **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.

118.1 **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

119. **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.

XIII - EXAMPLES OF TERRORIST FINANCING

120. 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

120.1. 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

120.2. 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

120.3. 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.

120.3A. 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.

120.3B. 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

120.4. 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

120.5. 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

120.6. 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

A. THE FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force's Forty Recommendations, issued in 1990, have been accepted worldwide as a comprehensive basis for tackling money laundering. The Recommendations were revised in 1996 to reflect "all serious crimes." The FATF has recently revised and updated the Forty Recommendations (2003); and has elaborated various Interpretative Notes which are designed to clarify the application of specific Recommendations and to provide additional guidance. An additional 8 "Special" Recommendations on Terrorist Financing were introduced in 2001. Special Recommendation 9 was introduced in 2004. The 40 Plus 9 Recommendations are relevant to all jurisdictions and are summarized below.

The FATF's 40 Special Recommendations (R):

R. 1 & 2. Money laundering should be criminalized on the basis of the UN's conventions and applied to all individuals and legal persons, determining as appropriate which serious crimes should be covered in addition to drugs.

R. 3. Appropriate measures should be put in place to confiscate the proceeds of crime.

R. 4. Banking secrecy laws must not conflict with or inhibit the effectiveness of the money laundering strategy.

R. 5-12 & 15. Administrative and regulatory obligations to develop systems and guard against money laundering should be imposed on all financial institutions.

R. 13 & 16. Obligations should be placed on all financial institutions, that, if they know or suspect or have reasonable grounds to suspect, that funds derive from criminal activity, they should report those suspicions promptly to the competent authorities.

R. 16, 20 & 24-25. The obligations for developing anti-money laundering systems, controls and reporting procedures should be applied to designated non-financial businesses and professions, recognizing, as appropriate, the concept of legal privilege.

R. 14. Financial and non-financial sector businesses, their directors and employees, should be protected against breach of confidentiality, if they report their suspicions in good faith.

R. 17. Appropriate, proportionate and dissuasive sanctions should be introduced for non-compliance with anti-money laundering or terrorist financing requirements.

R. 18. Countries should not approve the establishment or accept the continued operation of shell banks.

R. 19. Countries should consider implementing feasible measures to detect or monitor the physical cross-border transportation of cash and bearer-negotiable instruments, and should impose a requirement on financial institutions and intermediaries to report all transactions above a certain amount.

R. 21-22. Appropriate measures should be taken to ensure that financial institutions give special attention to business relationships and transactions whose anti-money laundering and anti-terrorist measures are inadequate.

R. 23-25. Countries should ensure that financial institutions, designated non-financial businesses and professions are subject to adequate regulation and supervision, and that criminals are prevented from owning and controlling financial institutions.

R.26-32. Appropriate law enforcement mechanisms should be put in place to process, investigate and prosecute suspected reports of money laundering, and an FIU should be established as the national receiving center for information on money laundering and terrorist financing.

R. 33 & 34. Countries should ensure the transparency of legal persons, and structures can be accessed on a timely basis.

R. 36-40. Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecutions and related proceedings, and provide the widest range of international co-operation to their foreign counterparts.

The FATF's 9 Special Recommendations:

Recognizing the vital importance of taking action to combat the financing of terrorism, the FATF has agreed these Recommendations, which, when combined with the FATF Forty Recommendations on money laundering, set out the basic framework to detect, prevent and suppress the financing of terrorism and terrorist acts.

I. Ratification and Implementation of UN Instruments

Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism as well as to immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

II. Criminalizing the Financing of Terrorism and Associated Money Laundering

Each country should criminalize the financing of terrorism, terrorist acts and terrorist organizations. Countries should ensure that such offences are designated as money laundering predicate offences.

III. Freezing and Confiscating of Terrorist Assets

Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organizations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts.

Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate 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.

IV. Reporting Suspicious Transactions Related to Terrorism

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organizations, they should be required to report promptly their suspicions to the competent authorities.

V. International Co-operation

Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organizations.

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, and should have procedures in place to extradite, where possible, such individuals.

VI. Alternative Remittance

Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF's Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions.

VII. Wire Transfers

Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.

Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers, which do not contain complete originator information (name, address and account number).

VIII. 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:

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

IX. Cash Couriers

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation. 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 or money laundering, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency bearer negotiable instruments are related to terrorist financing or money laundering, countries should also adopt measures, including legislative ones consistent with Recommendation 3 and Special Recommendation III, which would enable the confiscation of such currency or instruments.

B. THE UNITED NATIONS' CONVENTIONS

A number of UN conventions have been developed over the past two decades to deal with 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 Palermo Convention");
c) the United Nations Convention against Corruption; and
d) the United Nations Convention for the Suppression of the Financing of Terrorism.

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.

C. UNITED NATIONS RESOLUTIONS

The Security Counsel 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.

APPENDIX B

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 express use of foreign currency equivalents by the user/reader for purpose of adding clarity relative to such illustrations.

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.

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); and
- marketing and self-promotion.

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 with 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, 1999.

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's/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.

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 (eg. 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 Chapter 347 or the External Insurance Act Chapter 348.

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.

APPENDIX D

COLLECTION 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: *Contribution payments support organization*

Within a particular community, a terrorist organization requires a payment in order for a company to erect a new building. This payment is a known cost of doing business, and the construction company factors the payment into the cost of the project. If the company does not wish to pay the terrorist organization, then the project cannot be completed.

CASE 3: *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).

CASE 4: Loan and medical insurance policy scam used by terrorist group

An individual purchases an expensive new car. The individual obtains a loan to pay for the vehicle. At the time of purchase, the buyer also enters into a medical insurance policy that will cover the loan payments if he were to suffer a medical disability that would prevent repayment. A month or two later, the individual is purportedly involved in an "accident" with the vehicle, and the injury (as included

in the insurance policy) is reported. A doctor, working in collusion with the individual, confirms the injury. The insurance company then honors the claim on the policy by paying off the loan on the vehicle. Thereafter, the organization running the operation sells the motor vehicle and pockets the profit from its sale. In one instance, an insurance company suffered losses in excess of US$2 million from similar fraud schemes carried out by terrorist groups.

CASE 5: Credit card fraud supports terrorist network

One operation discovered that a single individual fraudulently obtained at least twenty-one Visa and MasterCard credit cards using two different versions of his name. Seven of those cards came from the same banking group. Debts attributed to those cards totaled just over US$85, 000. Such schemes also involved other manipulations of credit cards, including the skimming of funds from innocent cardholders. The latter method involved copying the legitimate cardholder's details from the magnetic strip onto duplicate cards, which were used to make purchases or cash withdrawals until the real cardholder discovers the fraud. The production of fraudulent credit cards has been assisted by the availability of programs through the Internet.

CASE 6: High account turnover indicates fraud allegedly used to finance terrorist organization

An investigation in Country B arose as a consequence of a suspicious transaction report. A financial institution reported that an individual who allegedly earned a salary of just over US$17,000 per annum had a turnover in his account of nearly US$ 356,000. Investigators subsequently learned that this individual did not exist and that the account had been fraudulently obtained. Further investigation revealed that the account was linked to a foreign charity and was used to facilitate the collection of funds for a terrorist organization through a fraud scheme. In Country B, the government provides funds to charities in an amount equivalent to 42 percent of donations received. Donations to this charity were being paid into the account under investigation and the government grant was being claimed by the charity. The original donations were then returned to the donors so that effectively no donation had been given to the charity. However, the charity retained the government funds. This fraud resulted in over US$1.14 million being fraudulently obtained.

CASE 7: Cash deposits and accounts of non-profit organization appear to be used by terrorist group

The FIU in Country L received a suspicious transaction report from a bank regarding an account held by an investment company. The bank's suspicions arose after the company's manager made several large cash deposits in different foreign currencies. According to the customer, these funds were intended to finance companies in the media sector. The FIU requested information from several financial institutions. Through these enquiries, it learned that the managers of the investment company were residing in Country L and a bordering country. They had opened accounts at various banks in Country L under the

names of media companies and a non-profit organization involved in the promotion of cultural activities.

The managers of the investment company and several other clients had made cash deposits into the accounts. These funds were ostensibly intended for the financing of media based projects. Analysis revealed that the account held by the non-profit organization was receiving almost daily deposits in small amounts by third parties. The manager of this organization stated that the monies deposited in this account were emanating from its members for the funding of cultural activities.

Police information obtained by the FIU revealed that the managers of the investment company were known to have been involved in money laundering and that an investigation was already underway into their activities. The managers appeared to be members of a terrorist group, which was financed by extortion and narcotics trafficking. Funds were collected through the non-profit organization from the different suspects involved in this case.

CASE 8: Individual's suspicious account activity, the use of CDs and a life insurance policy and inclusion of a similar name on a UN list

An individual resided in a neighboring country but had a demand deposit account and a savings account in Country N. The bank that maintained the accounts noticed the gradual withdrawal of funds from the accounts from the end of April 2001 onwards and decided to monitor the account more closely. The suspicions of the bank were subsequently reinforced when a name very similar to the account holder's appeared in the consolidated list of persons and entities issued by the United Nations Security Council Committee on Afghanistan (UN Security Council Resolution 1333/2000). The bank immediately made a report to the FIU.

The FIU analyzed that financial movements relating to the individual's accounts using records requested from the bank. It appeared that both of the accounts had been opened by the individual in 1990 and had been facilitated by mostly cash deposits. In March 2000 the individual made a sizeable transfer from his savings account to his chequing account. These funds were used to pay for a deposit single premium life insurance policy and to purchase certificates of deposit.

From the middle of April 2001, the individual made several large transfers from his savings account to his demand deposit account. These funds were transferred abroad to persons and companies located in neighboring countries and to other regions.

In May and June 2001, the individual sold certificates of deposit he had purchased, and transferred the profits to the accounts of companies based in Asia and to that of a company established in his country of origin. The individual also cashed in his life insurance policy before the maturity date and transferred its value to an account at a bank in his country of origin. The last transaction was carried out on 30 August 2001, that is, shortly before the September 11th attacks in the United States.

Finally, the anti-money laundering unit in the individual's country of origin communicated information related to suspicious operations carried out by him

and by the companies that received the transfers. Many of these names also appeared in the files of the FIU.

CASE 9: Front for individual with suspected terrorist links revealed by suspicious transaction report

The FIU in Country D received a suspicious transaction report from a domestic financial institution regarding an account held by an individual residing in a neighboring country. The individual managed European-based companies and had filed two loan applications on their behalf with the reporting institution. These loan applications amounted to several million US dollars and were ostensibly intended for the purchase of luxury hotels in Country D. The bank did not grant any of the loans.

The analysis by the FIU revealed that the funds for the purchase of the hotels were to be channeled through the accounts of the companies represented by the individual. One of the companies making the purchase of these hotels would have then been taken over by an individual from another country. This second person represented a group of companies whose activities focused on hotel and leisure sectors, and he appeared to be the ultimate buyer of the real estate. On the basis of the analysis within the FIU, it appeared that the subject of the suspicious transaction report was acting as a front for the second person. The latter, as well as his family, were suspected of being linked to terrorism.

CASE 10: Diamond trading company possibly linked to terrorist funding operation

The FIU in Country C received several suspicious transaction reports from different banks concerning two persons and a diamond trading company. The individuals and the company in question were account holders at the various banks. In the space of a few months, a large number of funds transfers, to and from overseas, were made from the accounts of the two individuals. Moreover, soon after the account was opened, one of the individuals received several US dollar cheques for large amounts.

According to information obtained by the FIU, one of the accounts held by the company appeared to have received large US dollar deposits originating from companies active in the diamond industry. One of the directors of the company, a citizen of Country C but residing in Africa, maintained an account at another bank in Country C. Several transfers had been carried out to and from other countries using this account. The transfers from foreign countries were mainly in US dollars. They were converted into the local currency and transferred to foreign countries and to accounts in Country C belonging to one of the two individuals who were the subject of the suspicious transaction reports.

Police information obtained by the FIU revealed that an investigation had already been initiated relating to these individuals and the trafficking of diamonds originating from Africa. The large funds transfers by the diamond trading company were mainly sent to the same person residing in another region. Police sources revealed that this person and the individual that had cashed the cheques

were suspected of buying diamonds from the rebel army of an African country and then smuggling them into Country C on behalf of a terrorist organization. Further research by the FIU also revealed links between the subjects of the suspicious transaction report and individuals and companies already tied to the laundering of funds for organized crime.

CASE 11: Lack of clear business relationship appears to point to a terrorist connection

The manager of a chocolate factory (CHOCCo) introduced the manager of his bank accounts to two individuals, both company managers, who were interested in opening commercial bank accounts. Two companies were established within a few days of each other, in different countries. The first company (TEXTCo) was involved in the textile trade, while the second one was a real estate (REALCo) non-trading company. The companies had different managers and their activities were not connected.

The bank manager opened the accounts for the two companies, which thereafter remained dormant. After several years, the manager of the chocolate factory announced the arrival of a credit transfer issued by REALCo to the account of TEXTCo. This transfer was ostensibly an advance on an order of tablecloths. No invoice was provided. However, once the account of TEXTCo received the funds, its manager asked for them to be made available in cash at a bank branch near the border. There, accompanied by the manager of CHOCCo, the TEXTCo manager withdrew the cash.

The bank reported this information to the FIU. The FIU's research showed that the two men crossed the border with the money after making the cash withdrawal. The border region is one in which terrorist activity occurs, and further information from the intelligence services indicated links between the managers of TEXTCo and REALCo and terrorist organizations action in that region.

CASE 12: Import/export business acting as an unlicensed money transmitter/remittance company

Suspicious transaction reports identified an import/export business with activity as an unlicensed money transmitter/remittance company, generating US$1.8 million in outgoing wire transfer activity during a five-month period. Wire transfers were sent to beneficiaries (individuals and businesses) in North America, Asia and the Middle East. Cash, cheques and money orders were also deposited into the suspect account totaling approximately US$1 million. Approximately 60 percent of the wire transfers were sent to individuals and businesses in foreign countries, which were then responsible for disseminating the funds to the ultimate beneficiaries. A significant portion of the funds was ultimately disseminated to nationals of an Asian country residing in various countries. Individuals conducting these transactions described the business as involved in refugee relief or money transfer. The individual with the sole signatory authority on the suspect account had made significant deposits (totaling US$17.4 million) and withdrawals (totaling US$56,900) over an extended period of time through what appeared to be 15 personal accounts at 5 different banks.

CASE 13: Use of cash deposits below the reporting threshold

A pattern of cash deposits below the reporting threshold caused a bank to file a suspicious transaction report. Deposits were made to the account of a bureau de change on a daily basis totaling over US$341,000 during a two and a half month period. During the same period, the business sent 10 wire transfers totaling US$2.7 million to a bank in another country. When questioned, the business owner reportedly indicated he was in the business of buying and selling foreign currencies in various foreign locations, and his business never generated in excess of US$10,000 per day. Records for a three-year period reflected cash deposits totaling over US$137,000 and withdrawals totaling nearly US$30,000. The business owner and other individuals conducting transactions through the accounts were nationals of countries associated with terrorist activity. Another bank made a suspicious transaction report on the same individual, indicating a US$80,000 cash deposit, which was deemed unusual for his profession. He also cashed two negotiable instruments at the same financial institution for US$68,000 and US$16,387.

APPENDIX E

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.

Bogus Property Company

As a result of the arrest of a large number of persons in connection with the importation of Cannabis from West Africa a financial investigation revealed that part of the proceeds had been laundered through a bogus property company, which had been set up by the traffickers in the UK. In order to facilitate the laundering process the traffickers employed a solicitor who set up a client account and deposited £500,000.00 received from them, later transferring the funds to his firm's bank account. Subsequently, acting on instructions, the solicitor withdrew the funds from the account and used them to purchase a number of properties on behalf of the defendants.

Theft of Company Funds

A fraud investigation into the collapse of a wholesale supply company revealed that the director had stolen very substantial sums of company funds laundering the money by issuing company cheques to third parties which were deposited into their respective bank accounts both in the UK and with offshore banks. Cheques drawn on the third party accounts were handed back to the director made payable to him personally. These were paid into his personal bank account. False company invoices were raised purporting to show the supply of goods by the third parties to the company.

Jersey Deposits and Sham Loans

Cash collected in the US from street sales of drugs was smuggled across the border to Canada where some was taken to currency exchanges to increase the denomination of the notes and reduce the bulk. Couriers were organized to hand carry the cash by air to London where it was paid into a branch of a financial institution in Jersey.

Enquiries in London by HM Customs and Excise revealed that internal bank transfers had been made from the UK to Jersey where 14 accounts had been opened in company names using local nominee directors. On occasions, the funds were repatriated to North America with the origin disguised, in the form of sham loans to property companies owned by the principals, either using the Jersey deposits as collateral or by transferring the funds back to North America.

Cocaine Lab Case

A disclosure was made by a financial institution related to a suspicious transaction which was based upon the fact that the client, as a non-account holder, had used the branch to remit cash to Peru, then having opened an account, had regularly deposited a few thousand pounds in cash. There was no explanation of the origin of the funds.

Local research identified the customer as being previously suspected of local cocaine dealing.

Production orders were obtained and it was found that his business could not have generated the substantial wealth that the customer displayed; in addition, his business account was being used to purchase chemicals known to be used in refining cocaine.

Further enquiries connected the man to storage premises which, when searched by police, were found to contain a cocaine refining laboratory, the first such discovery in Europe.

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.

Cash Deposits

Information was submitted about a customer who held two accounts at branches of the same financial institution in the same area. Although he was unemployed it was noted that he had deposited £500.00 – £600.00 cash every other day.

It was established that he held a third account and had placed several thousand pounds on deposit in Jersey. As a result of these investigations, he was arrested and later convicted for offences related to the supply of drugs.

Bank Complicity

Enquiries by the Police resulted in the arrest of a man in possession of 6 kgs of heroin. Further investigation established that an account held by the man had turned over £160,000.00 consolidated from deposits at other accounts held with the same financial institution. A pattern of transfers between these accounts, via the account holding branch, was also detected.

Information received led to a manager of the financial institution being suspected of being in complicity with the trafficker and his associates. He was arrested and later convicted of an offence of unlawful disclosure (tipping-off) and sentenced to four years imprisonment.

European Bank Pleads Guilty to Laundering in USA

The Case

Two South American nationals each opened an account at a European bank in February 1989. During the next year, approximately US$2.3 million was deposited in the accounts in the form of US cashiers cheques. The cashier's cheques were part of a smurfing operation in which money made from drug trafficking in California was used to purchase the cheques from various US banks. All these cheques were for less than US$10,000.00, which is the threshold limit for the filing of currency transaction reports (CTRs). After purchase, the cheques were sent to South America where they were aggregated and sent (in bulk) to the European bank for deposit. After the money had been deposited, approximately US$1.6 million was withdrawn and transferred back to the USA.

The Result

In December 1993, the European bank pleaded guilty to money laundering.

As part of the guilty plea, the bank admitted that the account officer who handled the accounts either knew or was willfully blind to the fact that these accounts were being used to launder the proceeds of crime.

The guilty plea was entered as part of a plea bargain under which the bank agreed to forfeit US$2.3 million to the US. In addition, the bank agreed to pay a fine of US$60,000.00, submit special audit reports for the following three years, and publish a document on money laundering for distribution to other European banks!

In Los Angeles, one of the two South Americans pleaded guilty to money laundering.

In addition to the US$2.3 million that the bank had agreed to forfeit, the US has confiscated a further US$1.75 million in real property and cash, which were traceable to the trafficking operation. The European Government has also confiscated US$1 million that was in the South Americans' accounts.

Suspicious New Business Venture for Respected Customer of Offshore Bank

The Case

An account manager with an international private bank (in one of the financial centers located in the English Channel) noticed that one of his customers had started to make cash deposits. The deposits were being made in batches through various bank branches in Birmingham. The customer's account had never received cash deposits, and the manager knew Birmingham sufficiently well to realize that all the bank branches in the city center were within easy walking distance of each other. The customer was a South African national living in the UK.

Whilst the deposits aroused the 'interest' of the manager, he did not necessarily feel that this amounted to suspicion. The valued customer had held the account for several years

and had, until this point, not given any cause for concern as to his legitimacy and respectability. The manager, therefore, wrote a 'customer care letter' indicating he had noticed the new cash deposits and enquired if the customer had started a new business venture; if so, could the bank assist him to process the cash deposits more efficiently and securely. The customer responded advising that he was starting a new venture importing second-hand electrical goods by air to the UK from his native South Africa; often the goods were to be paid for in cash, but he did not require any further services from his bank. The customer was more obliging than he realized for he enclosed with his response a copy of one of the airway bills by way of example!

The manager could not understand the commercial rationale for the importation, as surely the UK did not require second-hand electrical goods from South Africa and, even if it did, there was no sense in using expensive airfreight. Therefore a disclosure was made.

The Result

Investigations by HM Customs discovered that drugs were being imported to the UK packed in the electrical goods.

Points to Consider

- Unexpected changes in the pattern of transactions within long-established accounts may reveal valuable information. On-going monitoring of bank accounts is recommended in order to prevent fraud and money laundering.

- Further enquiries might be made of the customer if more information is needed to substantiate a suspicion by way of routine correspondence from the account executive responsible for the relationship. Such enquiries are not at risk from the tipping off offence as they are made **before** any decision is taken as to making a disclosure. They must not, however, refer in any way to suspicion or to the disclosure process, as this might tip off the customer. Such enquiries, where justified, do help to avoid unnecessary disclosures.

Verify Identity & 'Know Your Customer'

The Case

Three partners opened a business with a branch of a US bank in the UK. The partners were all American citizens, and one was resident in London. The bank followed rigorous 'know your customer' routines and, in line with group policies, also prepared a customer profile/template showing the pattern of transactions predicted from the information provided by the customers.

The partners explained that they were property developers, who were planning more business in the UK property market, hence the need for a local account. Therefore the customer profile/template predicted funds flowing to and from the USA and

disbursements within the UK. In reality, more than US$1 million was transferred into the account within a short period of time, all with instructions for immediate transfer to various accounts in Europe. There were few, if any, local UK disbursements.

A disclosure report was made.

The Result

The police were very interested and quickly made contact with the bank. At police request, the bank called in the customers in order to clarify details of the account, etc.

The police maintained observation and eventually arrested the customers.

Points to Consider

- It is not sufficient to merely verify identity. Institutions also need to know their customer and predict (however informal the prediction process may be) the customer's requirements and therefore the usual pattern of transactions through the account.

- A number of banks, especially US banks, are now preparing a new customer profile as an integral part of the new customer procedures for their banking business. The profile is considered of value from both the marketing and risk points of view. A predicted pattern of transactions would certainly help to identify the unusual/suspicious transactions, as it did in this case.

Insurance – Bank – Drug Trafficking

The Case

A drug trafficker bribed an insurance salesman to accept cash, contrary to company policy, to purchase a £200,000.00 single-premium policy.

The two co-operated on several occasions, each time involving large sums. On one occasion, the salesman put the cash into his own bank account and paid for the policy with his own cheque.

The case started before 1987, so there was no money laundering legislation at the time, but the operation continued after 1987. After 1987, the insurance company head office noticed the cash payments and queried them with the area manager who, after cursory enquiry of the salesman, advised head office that all was well.

To avoid the queries from head office, the salesman and drug trafficker opened their own bank account for the purpose of purchasing further policies for cash.

The bank manager was concerned and, following the second transaction after much hesitation, reported his suspicion.

The client's name was already known to HM Customs and Excise who were investigating the trafficker. The on-going Customs investigation revealed what was taking place.

The Result

Both the trafficker and the salesman were prosecuted under section 24 of the UK Drug Trafficking Offences Act for money laundering. Both received prison sentences. The Court confiscated the drug trafficker's funds, as was the salesman's commission from the trafficker, and also his commission from the insurance company on the sales of the policies.

Points to Consider

- The insurance company head office queried the purchases with the area manager who was receiving cascade commission on the sales made by the salesman. Did this influence the area manager's enquiry?
- Any enquiries by the reporting officer should be made of uninvolved members of management and of the basic documentary records.
- The insurance company failed to identify the purchase of the policy for a named client by the salesman concerned. Fraud prevention as well as money laundering should call for this type of transaction to be queried.
- The salesman's bank failed to enquire as to the large cash deposit followed by a cheque to the insurance company through the salesman's account. (This happened before 1987 – it is to be hoped that it would not happen now.)
- The bank became suspicious of the joint account because there was difficulty in verifying the identity of one of the parties and because of the nature of the transactions.

Insurance Company Disclosure Pays Unexpected Dividends

The Case

A financial disclosure report from an insurance company directly resulted in police uncovering a major theft of bank notes from a financial institution.

An insurance company became suspicious when offered cash to buy an insurance bond. There were two occasions, the first involving £30,000.00 and the second involving £100,000.00. The insurance company head office noted that members of the two families involved were employed at the same financial institution.

The police investigated 9 suspects.

One employee convicted of theft was paid £1,200.00 - £1,500.00 per month; the Court were advised that he stole £170,000.00. The employee used the proceeds to pay off his £37,000.00 mortgage on his home, put down £45,000.00 deposit on a new one, pay for £6,700.00 holiday in The Seychelles, buy a Land Rover Discovery, and to make expensive extensions and additions to the family home.

It would appear that the bank notes were initially hidden in a wardrobe, and the money not spent was subsequently paid into a building society account.

The Result

Production orders were served on the bank and building society accounts of the suspects, and nine people were arrested. Eventually, one person pleaded guilty and was imprisoned, but because no theft could be proven, the other cases were not proceeded with. However, a number of civil actions were taken against those involved.

Points to Consider

- Large sums of cash being used to buy retail investment products are sufficiently unusual to alert an institution to a possible problem. Some institutions have implemented policies of not accepting cash, or not accepting cash up to a financial threshold, or insisting that all cash transactions accepted are reported to the Money Laundering Reporting Officer for review.
- Motor dealers offered cash for expensive cars should consider the source of the cash and the address of the purchaser (known through completion of the 'log book'). If, as is suggested in this case, the quality of the vehicle and the amount of cash do not appear to match the address, then motor-traders should remember their obligations under the substantive law. In other words, they should report suspicions.
- Unexpected redemption of mortgages in cash should raise an enquiry.
- Large cash deposits to open a building society or bank account should also raise an enquiry.

The Cost of Getting It Wrong

The Case

Bank staff made an internal report to the Money Laundering Reporting Officer about a customer's account, where the debit/credit turnover (cash and cheque) was considered excessive in view of the customer's salary. The Money Laundering Reporting Officer considered that the circumstances did not warrant disclosure, but requested that the account be kept under review and a further report be submitted.

A further report was submitted a few months later based upon similar justification, but additionally indicating that the customer was a frequent traveler and had used his debit card in a number of countries, including Holland and Indonesia. The Money Laundering Reporting Officer, relying on the search carried out by the staff, decided to make a disclosure.

The customer was a solicitor employed by a local authority. A police officer (not within the Financial Investigation Unit) made enquiries of the customer's employer (specifically, the chief executive and director to whom the customer reported). Although the officer was assured that his enquiries would be treated confidentially, the customer's line manager decided that the issues were too serious to ignore and raised them with the employee.

The employee demanded to know the source of the allegations, and agreed to explain the 'suspicious' transactions on his statements only if the source of the allegations was disclosed to him.

The employee then complained to the bank, and sought compensation for damage to reputation, etc. The initial complaint was addressed to the branch by both telephone and letter, but the branch felt that it could not respond for fear of triggering the tipping off offence. This apparent lack of co-operation only increased the customer's irritation.

The bank rejected the claim, stating that their statutory obligation to report overrides the obligation to customer confidentiality.

The customer rejected this argument, claiming that the banking practice required due care and attention and due diligence prior to making a disclosure. He argued that reasonable internal enquiries would have removed such suspicion. He emphasized the fact that had the bank taken trouble to examine the 'suspicious transaction' with sufficient care they would have seen that:

(a) one cheque credited was from another part of the same banking group;

(b) another cheque credited was from his employer;

(c) the drawers of other cheques credited were other reputable financial institutions; and,

(d) cash transactions were infrequent and isolated.

In addition, he contended that the bank had no right or obligation to disclose details of his salary or any other transaction about which they were not suspicious.

Following "deadlock" between the bank and the customer, the customer took his complaint to the banking Ombudsman, who agreed to examine the case.

The bank undertook further internal enquiries as to the circumstances of the disclosure, and also took legal advice. Legal advice (and hindsight) challenged:

(a) whether the credit/debit turnover was really excessive, as during the period overall the bulk of the movements had been of his salary;

(b) the change of attitude and decision by the Money Laundering Reporting Officer, as there had been little significant change of circumstance between the first internal report and the second; and,

(c) the degree of skill and care applied by the staff, as available internal information (especially cheque drawer information) gave sufficient information about the source of funds to remove suspicion.

The Result

Having taken legal advice, the bank concluded that they might be in difficulty if they allowed the matter to proceed to the Ombudsman or even the Court, on the grounds that had staff undertaken an examination of the source of the funds, their suspicions might have been allayed and no report would have been made. The bank therefore paid modest compensation to the customer. The police apologized to the bank for their incorrect handling of the case and for the excessive zeal of the untrained officer.

Points to Consider

Despite the safeguards, there will be rare occasions when the customer (the innocent customer) becomes aware of the disclosure because of police or customs enquiries.

Provided the person submitting the report is subjectively suspicious, the immunity from breach of confidentiality applies. There is no need for objective criteria to support the suspicion. However, the statutory defence would not necessarily protect somebody who made a disclosure carelessly.

Financial institutions must carefully consider how extensive an internal enquiry the Money Laundering Reporting Officer/institution should carry out to be sure that all factual information available that might negate a suspicion has been examined.

Police forces must observe their commitment to financial institutions, and should never allow any officer other than a trained financial investigator to handle financial disclosures.

The customer's line manager was guilty of tipping off and, had the bank's suspicions been substantiated and the case been proved, he could have been prosecuted for this offence. A financial institution may find itself in a similar situation if it becomes aware that one of its own employees is under investigation. Two ways spring to mind as to how this might occur. Firstly, an institution might make a disclosure about an employee. Secondly, the institution might learn of an investigation into the employee – possibly on receipt of a production order. If, as in this case, the suspected employee holds a responsible position or has access to value

etc., the institution may feel that it needs to take action to protect its position. Wherever this occurs, it is imperative that the institutions discuss their situation with the senior officer of the Financial Investigation Unit team in order to agree to the course of action.

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:

Suspicious 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

APPENDIX G

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 ☐
- Drug Trafficking ☐
- Terrorism Finance ☐
- Other ☐

Report No.:.....
Type of Transaction: .....
.....
……..

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: .....

.....

.....

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

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

[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

Details of Sums Arousing Suspicion Indicating Debit or Credit Source and Currency Used	Amount	Debit or Credit	Date	Source	Currency

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.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Submitted By: _____ Signature: _____

Position Held:_____

You are asked to assist with completing the attached statistical analysis, which will help us to give you feedback – Thank you!

STATISTICAL INFORMATION

Nature of Institution	**Please tick**	**Grounds for Disclosure?** *Please tick all that apply*	**Please tick**
Bank		Media / Publicity	
Fund Manager		Internet Research	
Bureaux Des Changes		Group Information	
Stockbroker		3rd Party Information	
Financial Advisor		Service of Production, Charging or Monitoring Order	
Insurance Company		Police enquiry	
Trust Company		Account Activity Not in Keeping with KYC	
Corporate Service Provider		Evidence of Forged Documentation	
Lawyer		Cash Transactions	
Accountant		Transitory Accounts – Immediate Layering	
Casino		High Risk Jurisdictions	
Real Estate Agent/Broker		Purchase and Surrender of Insurance Policy	
Credit Union		Unusual Forex Transactions	
Alternative Remittance		Repeat disclosures	
Local Regulator		Failure to comply with due diligence checks	
Other Regulator		Other (specify)	
Other (specify)			
		What currency was involved?	
Customer/Transaction Type		GBP	
Involving at least one intermediary		USD	
Long Standing Customer		EUR	
New Customer		CAD	
Electronic Banking		JPY	
EURO Transaction		MXN	
		BRL	
		SEK	
Criminality Suspected		CHF	
Drugs		BSD	
Terrorism		OTHER	
Fraud			
Revenue Fraud			
Insider Dealing			
Corruption			
Unknown / undetermined			
Regulatory Matters			
Other			

Completed forms should be forwarded 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, Fax No: (242) 322-5551

APPENDIX H

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

Your Ref:
Our Ref: Date:

...200X

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,

Anthony M. Johnson

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

Your Ref:
Our Ref: **Date:** **200X**

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,

Anthony M. Johnson

Director

Financial Intelligence Unit

APPENDIX I

SOURCES UTILIZED IN PREPARING THE GUIDELINES

1. ***The New Financial Legislative Regime: An Explanatory Note*** **by Lennox Paton Counsel and Attorneys-At-Law, Nassau, Bahamas.**

2. ***Guidance Notes on the Prevention of Money Laundering and Countering The Financing of Terrorism*** **by the Guernsey Financial Services Commission.**

3. ***Money Laundering and Terrorist Financing Prevention and Compliance - Reporting Officer's Reference Guide 2006*** **by BBA Enterprises Ltd and Michael Hyland Associates.**

4. ***Guidelines for Licensees on the Prevention of Money Laundering & Countering the Financing of Terrorism*** **by the Central Bank of The Bahamas.**

5. **Federal Financial Institutions Examination Council *Bank Secrecy Act/Anti-Money Laundering Examination Manual,* USA.**

6. ***Capacity Enhancement Program on Anti-Money Laundering and Combating the Financing of Terrorism Workbook*** **by the World Bank.**

7. ***40 + 9 Recommendations*** **by the Financial Action Task Force.**

8. **Serious Organized Crime Agency (SOCA), U.K.**

9. **Financial Crimes Enforcement Network (FinCEN), USA.**