SUSPICIOUS TRANSACTIONS AND ANTI-MONEY LAUNDERING GUIDELINES

FOR THE INSURANCE SECTOR IN THE BAHAMAS

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

EXPLANATORY FOREWORD

The Financial Intelligence Unit of The Bahamas is empowered by section 15 of the Financial Intelligence Unit Act, 2000 (Act No. 30 of 2000) to issue suspicious transaction and anti-money laundering guidelines, from time to time, in respect of each category of financial institution to which the Financial Transactions Reporting Act, 2000 (Act No. 40 of 2000) applies and to amend or revoke such guidelines from time to time. These guidelines are formulated to outline the requirements of the Financial Transactions Reporting Act, 2000, the Financial Transactions Reporting (Amendment) Act, 2001 (No. 17 of 2001), the Financial Transactions Reporting Regulations, 2000 (Statutory Instrument No. 111 of 2000), the Financial Transactions Reporting (Amendment) Regulations, 2001 (Statutory Instrument No. 113 of 2001), the Proceeds of Crime Act, 2000 (Act No. 44 of 2000), the Financial Intelligence Unit Act, 2000 the Financial Intelligence Unit (Amendment) Act, 2001 (Act No. 20 of 2001) and the Financial Intelligence (Transactions Reporting) Regulations, 2001 (Statutory Instrument No. 7 of 2001) to provide a practical interpretation of the provisions of the legislation and to give examples of good practice.

The Proceeds of Crime Act, 2000 repealed the Money Laundering (Proceeds of Crime) Act, 1996, as well as the Tracing and Forfeiture of Proceeds of Drug Trafficking Act, (Chapter 86). The Proceeds of Crime (Money Laundering) Regulations, 2001 (Statutory Instrument No. 8 of 2001) repealed the Money Laundering (Proceeds of Crime) Regulations, 1996 (Statutory Instrument No. 69 of 1996).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

This document contains guidelines, which are intended to be illustrative of best industry practice for a company carrying on life assurance business as defined in section 2 of the Insurance Act, Chapter 317 and the External Insurance Act, Chapter 318 and persons dealing in life assurance policies and certain classes of general insurance business.

Additionally, the Financial Intelligence Unit has issued Guidelines specifically for the following sectors:

- banks and trust companies within the meaning of the Central Bank Of The Bahamas Act, 2000 (Act No. 37 of 2000) and the Banks and Trust Companies Regulation Act, 2000 (Act No. 38 of 2000);
- person's registered by the Securities Commission within the meaning of the Securities Industry Act, 1999, (Act No. 1 of 1999) and all licensed and unlicensed mutual funds administrators or operators, within the meaning of the Mutual Funds Act, 1995 (Act No. 6 of 1995);
- licensed casino operators, within the meaning of the Lotteries and Gaming Act, 1987, Chapter 351;
- co-operative societies registered under the Co-operative Societies Act, Chapter 284; and,
- other financial services providers reported to in 3(1) of the Financial Transactions Reporting Act, 2000.

Should an institution to which these Guidelines apply adopt alternative procedures relating to its anti-money laundering policies and practices, that institution will be required to demonstrate the adequacy of those procedures.

The courts shall have regard to any relevant Guidelines issued by the Financial Intelligent Unit or the relevant agency or both.

SUSPICIOUS TRANSACTIONS AND ANTI -MONEY LAUNDERING GUIDELINES FOR THE INSURANCE SECTOR

SCOPE

These Guidelines have been prepared in consultation with the Registrar of Insurance Companies, and those financial institutions and industry organisations that expressed an interest in being consulted in the course of the development of these Guidelines. The scope of these Guidelines covers all mainstream insurance business as defined in the Insurance Act and the External Insurance Act Chapters 317 and 318 respectively, Statute Laws of The Bahamas, 1987 Edition.

However, where a Bahamian financial institution engaged in the insurance sector is a part of an international group, it is recommended that a group policy be established to the effect that all overseas branches and subsidiaries ensure that verification of identity and record keeping practices are undertaken at least to the standards required under Bahamian law or, if standards in the host country are considered or deemed more rigorous, to those higher standards. Reporting procedures and the offences to which the money laundering legislation in The Bahamas relates must be adhered to in accordance with Bahamian laws and practices.

SUSPICIOUS TRANSACTIONS AND

ANTI-MONEY LAUNDERING GUIDELINES FOR

THE INSURANCE SECTOR

SUSPICIOUS TRANSACTIONS AND

ANTI-MONEY LAUNDERING GUIDELINES FOR

THE INSURANCE SECTOR

I - BACKGROUND

1 The Bahamian law relating to money laundering is contained in the Proceeds of Crime Act, 2000 the Financial Transactions Reporting Act, 2000 and the Financial Intelligence Unit Act, 2000. This legislation together with the Financial Transactions Reporting Regulations, 2000, and the Financial Intelligence (Transactions Reporting) Regulations, 2001 are summarised in Appendix B.

WHAT IS MONEY LAUNDERING?

2 Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it also allows them to maintain control over those proceeds and, ultimately, to provide a legitimate cover for their source of income (see sections 40, 41 and 42 of the Proceeds of Crime Act, 2000).

THE NEED TO COMBAT MONEY LAUNDERING

3 In recent years, there has been a growing recognition that it is essential to the fight against crime that criminals be prevented, whenever possible, from legitimising the proceeds of their criminal activities by converting funds from “dirty” to “clean”.

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

5 Thus, The Bahamas, as a large financial centre, has an important role to play in combating money laundering. Financial institutions that knowingly become involved in money laundering, risk prosecution and

the loss of their entitlement to operate within or from The Bahamas.

STAGES OF MONEY LAUNDERING

6 There is no one method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g., cars or jewelry) to passing money through a complex international web of legitimate businesses and "shell" companies. Initially, however, in the case of drug trafficking and other serious crimes enforceable under the Proceeds of Crime Act, 2000, the proceeds usually take the form of cash, which needs to enter the financial system by some means.

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

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

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

c) Integration - the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

8 The three basic steps may occur as separate and distinct phases. They may occur simultaneously or, more commonly, they may overlap. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminal organisations. Appendix F provides some typical examples.

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

- entry of cash into the financial system;
- cross-border flows of cash; and,
- transfers within and from the financial system.

VULNERABILITY OF FINANCIAL INSTITUTIONS ENGAGED IN INSURANCE BUSINESS TO MONEY LAUNDERING

10 Efforts to combat money laundering largely focus on those points in the process where the launderer's activities are more susceptible to recognition and have, therefore, to a large extent concentrated on the deposit taking procedures of financial institutions; i.e., the placement stage. Equally, however, it is emphasised that there are also many crimes (particularly the more sophisticated ones) where cash is not involved.

11 Although it may not appear obvious that insurance products might be used for money laundering purposes, vigilance is necessary throughout the financial system to ensure that non-traditional financial services products are not exploited.

12 Insurance service providers who deal directly with the public may be used at the initial placement stage of money laundering, particularly if they receive cash. Premiums on insurance policies may be paid in cash, with the policy subsequently being cancelled in order to get a return of premium, or an insured event may occur resulting in a claim being paid out.

13 Lump sum investments in liquid products are clearly most vulnerable to use by money launderers, particularly where they are of high value. Payment in cash is likely to merit further investigation, particularly where it cannot be supported by evidence of a cash-based business as the source of funds.

14 Financial institutions involved in insurance business should therefore keep transaction records that are comprehensive enough to establish an audit trail.

II - WHAT THE BAHAMIAN LAW REQUIRES

THE BAHAMIAN LAW

15 The Bahamian law relating to money laundering is contained in the following legislation:

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

THE PROCEEDS OF CRIME ACT, 2000

This Act criminalizes money laundering related to the proceeds of drug trafficking and other serious crimes. 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.

The law requires financial institutions to inform the Financial Intelligence Unit or a Police officer authorized to receive the 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

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

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

The Financial Intelligence Unit Act, 2000 establishes the Financial Intelligence Unit of The Bahamas, which has power, inter alia, to obtain, receive, analyse and disseminate information, which relates to or may relate to offences under the Proceeds of Crime Act, 2000.

THE FINANCIAL INTELLIGENCE (TRANSACTIONS REPORTING) REGULATIONS, 2001

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. 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.

MONEY LAUNDERING OFFENCES, PENALTIES AND DEFENCES: THE PROCEEDS OF CRIME ACT, 2000 AND THE FINANCIAL TRANSACTIONS REPORTING ACT, 2000

16 CONCEALING, TRANSFERRING OR DEALING WITH THE PROCEEDS OF CRIMINAL CONDUCT

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

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.

17 ASSISTING ANOTHER TO CONCEAL THE PROCEEDS OF CRIMINAL CONDUCT

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 serious criminal conduct or any relevant offence.

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. It is important to note that these are mandatory penalties.

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 serious 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.

18 ACQUISITION, POSSESSION OR USE

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.

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. It is important to note that these are mandatory penalties.

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.]

19 FAILURE TO DISCLOSE

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 and such information or the matter on which the information is based came to his attention in the course of his trade, profession, business or employment.

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.

Defence: It is a defence 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.

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.

(*See a* summary of the legislation in Appendix B of these Guidelines.)

Financial Transactions Reporting Act, 2000

This legislation 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 Proceed 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.

The Suspicious Transaction Report (STR) should be made in writing containing 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.

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.

20 TIPPING OFF

It is also an offence for anyone who knows suspects or has reasonable grounds to suspect that a disclosure has been made, 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 authorised agency and it becomes necessary to make further enquiries, great care should be taken to ensure that customers do not become aware that their names have been brought to the attention of the authorities.

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.

(See Appendix B of these Guidelines).

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.

Financial Transactions Reporting Act, 2000

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 knowingly disclose that information to any other person, to obtain an advantage or a pecuniary gain or to prejudice the investigation.

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

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.

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

- Internal controls, policies and procedures (Section III]
- Identification procedures (Section IV);
- Record keeping (Section V);
- Suspicious transactions reporting procedures (Section VI);
- Appointment of a Money Laundering Reporting Officer (Section VI);
- Education and training of employees in the procedures, laws and detection of suspicious transactions (Section VII).

21 **Important Definitions**

The term "criminal conduct" includes -

(1) drug trafficking;

(2) bribery and corruption;

(3) money-laundering;

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

(5) an offence committed anywhere that, if committed in The Bahamas, would constitute an offence in The Bahamas as set out in the Schedule to the Proceeds of Crime Act, 2000.

The following terms are also defined for ease of reference -

"facility" means any account or arrangement that is provided by a financial institution to a facility holder and by, through or with which the facility holder may conduct two or more transactions whether or not they are so used. It specifically includes provision of facilities for safe custody, including safety deposit boxes;

a "facility holder" is the person in whose name the facility

is established and includes any person to whom that facility is assigned or who is authorised to conduct transactions through that facility;

an "occasional transaction" is a cash transaction that involves a payment, deposit, withdrawal, debit, repayment,

encashment, exchange, or transfer of cash that is conducted by any person otherwise than through a facility of which that person is a facility holder;

"cash" means any coin or paper money that is designated as legal tender in the country of issue and includes bearer bonds, travellers cheques, postal orders and money orders.

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

RESPONSIBILITIES OF THE RELEVANT AGENCIES/ SUPERVISORY AUTHORITES

22 The fact that financial services providers are vulnerable to money laundering means that the Registrar of Insurance, as regulator of financial institutions engaged in insurance business licensed under the Insurance Act and the External Insurance Act, Chapters 317 and 318 respectively, maintains a keen interest in measures aimed at countering money laundering.

23 The Registrar of Insurance expects its licencees to instruct their external auditors to submit a report during the course of the annual audit of financial statements on the adequacy of policies and procedures relating to money laundering specified in the Financial Transactions Reporting Regulations, 2000. A copy of such report must be forwarded to the Registrar of Insurance, within four months of the end of the financial year.

24 The Registrar of Insurance monitors financial institutions licensed under the Insurance Act and the External Insurance Act, Chapters 317 and 318 respectively, for their compliance with policies, procedures and controls relating to money laundering activities through prudential discussions, internal and/or external audit reports and/or management review reports.

25 The Proceeds of Crime Act, 2000 and the Financial Transactions Reporting Act, 2000, together require the supervisory authorities of financial institutions themselves to report any information they obtain which in their opinion indicates that any person has or may have been engaged in money laundering and to disclose that information to the Financial Intelligence Unit or the law enforcement authorities.

III - INTERNAL CONTROLS, POLICIES AND PROCEDURES

26 Insurance sector institutions are legally obligated to establish, implement and maintain policies, procedures, and controls which deter criminals from using their facilities for money laundering.

27 Insurance sector institutions are required to establish a central point of contact with the Financial Intelligence Unit in order to handle the reported suspicions of their staff regarding money laundering. Such institutions are required to appoint a "Money Laundering Reporting Officer" to undertake this role, and such officer is required to be registered with the Financial Intelligence Unit. Such institutions are also required to appoint a "compliance officer" who shall ensure full compliance with the laws of The Bahamas. (see regulation 5(e) of the Financial Intelligence (Transactions Reporting) Regulations, 2001).

28 All insurance sector institutions licensed to operate within or from The Bahamas are required to:

i. introduce procedures for the prompt validation of suspicions transactions and subsequent reporting to the Financial Intelligence Unit;

ii. provide the Money Laundering Reporting Officer with the necessary access to systems and records to fulfill this requirement; and,

iii. establish close co-operation and liaise with the Registrar of Insurance (see Section VI of these Guidelines).

29 An Insurance sector institutor may choose to combine the roles of the Compliance Officer and the Money Laundering Reporting Officer, depending upon the scale and nature of business. The roles might be assigned to its Internal Audit or Compliance Department.

30 The Legislation places an obligation on all insurance sector institutions from time to time to comply with policies, procedures, and controls relating to money laundering activities to satisfy the requirements of the Financial Transactions Reporting Regulation, 2000 and the Financial Intelligence (Transaction Reporting) Regulations, 2001. Larger insurance sector institutor may wish to assign this role to their Internal Audit or Compliance Departments. Smaller institutions may wish to introduce a regular review by management.

IV - IDENTIFICATION PROCEDURES

INTRODUCTION

31 The Financial Transactions Reporting Act, 2000 requires financial institutions (which is defined to include insurance sector institutions) to verify the identity of persons requesting use of their facilities. Verification of identity is mandatory (see Appendix A for specific offences and penalties).

WHEN MUST IDENTITY BE VERIFIED

32 Sections 6, 7, 8 and 9 of the Financial Transactions Reporting Act, 2000 provides inter alia that financial institutions must verify the identity of the following persons:

- persons who wish to become facility holders; verification must be completed before they become a facility holder;

- each and every existing facility holder (verification to be completed within twelve months of the coming into force of the Financial Transactions Reporting Act, 2000). This period may be extended by an additional period of twelve months by order of the Minister. NB: If at the end of the prescribed period the financial institution is still unable to verify the identity of the facility holder, the financial institution shall assign the facility to the Central Bank of The Bahamas in accordance with section 16 of the Banks and Trust Companies Regulation Act, 2000;

- where the identity of an existing facility holder is doubtful, the financial institution is required to verify the identity of the facility holder;

- whenever an occasional transaction or series of linked transactions are undertaken (see paragraphs 36-38 below) and the total amount of the cash involved exceeds $10,000.00, the identity of the prospective customer must be verified. Once identification procedures have been satisfactorily completed, then the business relationship may be established and as long as records are maintained in accordance with the Financial Transactions Reporting Act, 2000, no further evidence of identity is needed when transactions are subsequently undertaken; and,

- where an occasional transaction is conducted on behalf of a third party, or where the financial institution has reasonable grounds to

believe that an occasional transaction is being conducted on behalf of a third party and the total amount of the cash involved exceed $10,000.00, the financial institution is required to verify the identity of the third party (see summary of legislation in Appendix B).

33 There is a general obligation to maintain procedures for obtaining evidence of identity, but section 6(5), 10 and 11(5) of the Financial Transactions Reporting Act, 2000 and regulation 5A of the Financial Transactions Reporting Regulations, 2000 set out a number of exemptions from this requirement.

Additionally, sections 7(2), 8(6) and 9(6) provide instances where, inter alia, one financial institution may rely on written confirmation of identity from another financial institution. Irrespective of these exemptions (set out below) identity must be verified in all cases where money laundering is known or suspected and the details reported in line with the procedures set out in Section VI of these Guidelines.

IDENTIFICATION PROCEDURES: EXEMPTIONS

The Financial Transactions Reporting Act, 2000, permits a financial institution to rely on the written confirmation of another financial institution that the latter has verified the identity of a customer, section 2(3) of the Act restricts the definiation of "financial institution" to include only five of the institutions listed in section 3 of the Act, namely, banks and trust companies; companies carrying on life assurance business; licensed casino operators; broker dealers and mutual fund administrators or operators of mutual funds (see section 3(1)(a), (b), (e), (f) and (i)).

The obligation to verify is general, but the law does permit a number of exemptions from this general requirement. Insurance sector participants should identify which exemptions apply to them.

34 These exemptions are-

(i) <u>Superannuation Schemes</u>

Where a request is made to a trustee or administration manager or investment manager of a superannuation scheme which permits public participation, for a person to become a facility holder, the identity of such applicant does not have to be verified if either, he becomes a member of the scheme because of the transfer to that scheme of all the members of another superannuation scheme; or he becomes a member of a section of that scheme because of the transfer to one section of that scheme, of all the members of another section of the same scheme.

(ii) Discretionary Trusts

There is no requirment to verify the identity of any beneficiary under a trust who has vested interest, and the transaction is being, or has been, conducted on that person's behalf in his or her capacity as such beneficiary.

(iii) Occupational Retirement/Pension Plans which allow non-employee participation

There is no requirement to verify the identity of any person who has become or is seeking to become a member of a supperannuation scheme which is established principally for the purpose of providing retirement benefits to employees. The trustee or manager is deemed to have complied with the requirements to verify the identity of that person if that person's identity has been verified by his or her employer.

(iv) Government Agencies

Documentary evidence of identity will not normally be required if the client is a central or local government, statutory body or agency of the Government.

(v) Other Financial Institutions/Entitities

Regulation 5A of the Financial Transactions Reporting Regulations, 2000, provides that no documentary evidience would normally be required for verification of the identity of the following financial insitutions and other entities-

(i) financial institutions regulated by the Central Bank of The Bahamas, the Securties Commission of The Bahamas, the Registrar of Insurance of The Bahamas or the Gaming Board of The Bahamas;

(ii) financial institutions located in the jurisdictions specified in the First Schedule of the Financial Transactions Reporting Act, 2000 which are regulated by a body with equivalent regulatory and supervisory responsibilities to those bodies listed in paragraph (i) above;

(iii) any Central or local government agency or statutory body;

(iv) a publicly traded company or mutual fund listed on The Bahamas International Stock Exchange or any of the Stock Exchanges specified in theSchedule to the Regulations and approved by the Securities Commission of The Bahamas;

(v) a regulated mutual fund in The Bahamas or a mutual fund located in any juridiction specified in the First Schedule of the Financial Transactions Reporting Act, 2000 which is

regulated by a body with equivalent regulatory and supervory responsibilities as the Securities Commission of The Bahamas;

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

(vii) an applicant for insurance in respect of which a premium is payable in one instalment of an amount not exceeding $2,500.00;

(viii) an applicant for insurance in respect of which a periodic premium is payable and where the total payable in respect of any calender year does not exceed $2,500.00.

35. Reliance may be placed by one financial institution on the written confirmation of a customer's identity provided by another financial institution in The Bahamas or a foreign finanical institution in the following cases:

(i) Section 7(2) of the Financial Transactions Reporting Act, 2000 provides that where any person conducts an occasional transaction by, through, or with a financial institution, that financial institution, is not required to verify the identity of such a person in any case where -

- the financial institution is unable to readily determine whether or not the transaction involves funds because the funds involved in the transaction are deposited by the person into a facility (being a facility in relation to which that financial institution is a facility holder) provided by another institution; and,

- the financial institution has obtained written confirmation that the other financial institution has verified the identity of the person.

(ii) Section 8(6) of the Financial Transactions Reporting Act, 2000 provides that where a financial institution, as defined in section 2(3) of the Financial Transactions Reporting Act, 2000, confirms that it has verified the identity of a person or persons for whom it is conducting an occasional transaction by, through, or with another financial institution, that other financial institution, having obtained the said written confirmation, is not required to verify the identity of the person or persons for whom the transaction is being conducted.

(iii) Section 9(6) of the Financial Transactions Reporting Act, 2000 provides that where a financial transaction is conducted on behalf of a third party through the facilities of a financial institution as

defined in section 2(3) of the Act, that institution ("A") is not required to verify the identity of the third party if -

- the transaction is conducted by another financial institution (which falls within section 3(1)(a), (b), (e), (f) and (i)) ("B") on behalf of a person or persons; and

- ("A") has obtained from ("B") written confirmation that ("B") has verified the identity of the person or persons on whose behalf ("A") is conducting the transaction.

OCCASIONAL TRANSACTIONS: SINGLE OR LINKED

36 The need to aggregate linked transactions is designed to identify those who might structure their business to avoid the identification procedures, and is not meant to cause inconvenience to genuine business. There is clearly no need to double up both ends of the same transaction.

37 The Financial Transactions Reporting Regulations, 2000 do not require insurance sector institutions to establish additional systems specifically to identify and aggregate linked transactions. However, if an insurance sector institution existing systems recognise that two or more transactions have totalled more than $10,000.00 then this information must be acted upon as soon as practicable after it comes to the attention of the financial institution.

INTRODUCTION OF OCCASIONAL TRANSACTIONS FROM OVERSEAS

38 Where a person who is conducting an occasional transaction, is introduced by a foreign financial institution, as defined in section 2(3) of the Financial Transactions Reporting Act, 2000, from a First Schedule country (see Appendix E), the proviso to section 8(6) of the Financial Transactions Reporting Act, 2000 provides that the financial institution to whom the introduction is being made, need not verify identity and may accept written confirmation that evidence of identity has been taken and verified by the foreign financial institution.

VERIFICATION PROCEDURES: INTRODUCTION

39 In circumstances other than those set out in paragraphs 34-38 above, identity must be verified. The Financial Transactions Reporting Act, 2000 and the Financial Transactions Reporting Regulations, 2000 specify what evidence of identity is required.

40 A financial institution should establish to its satisfaction that it is dealing with a person (natural or corporate) and verify the identity of those persons who have use of insurance products and services.

41 Whenever possible, the prospective customer should be interviewed personally.

42 Section 11(2) of the Financial Transactions Reporting Act, 2000 provides that in verifying the identity of any person, a financial institution may rely (in whole or in part) on evidence used by that financial institution on an earlier occasion to verify that person's identity, if the financial institution has reasonable grounds to believe that the evidence is still reasonably capable of establishing the identity of that person.

43 Section 11(3) of the Financial Transactions Reporting Act, 2000 provides that where a financial institution, as defined in section 2(3) of the Financial Transactions Reporting Act, 2000, is required by any provision of Part II of the Act, to verify the identity of any person in relation to any facility; and transactions may be conducted through that facility by means of an existing facility held by the person as a facility holder in another financial institution, and the first mentioned financial institution has obtained confirmation in writing that the other financial institution has verified the identity of the person, then the first mentioned financial institution shall be deemed to have complied with the requirement to verify the identity of that person if that financial institution takes all such steps as are reasonably necessary to confirm the existence of the other facility.

In other words, in the case of arrangements between two facilities which accommodate the conduct of transactions between them (whether held by the same of different financial institutions), the duty to verify identity is met once all such steps as are reasonably necessary to confirm the existence of the other facility have been taken.

44 Section 11(4) of the Financial Transactions Reporting Act, 2000 provides that where a financial institution, as defined in section 2(3) of the Financial Transactions Reporting Act, 2000, confirms in writing that it has verified the identity of a person in relation to an occasional transaction which is conducted by means of an existing facility that is provided by another financial institution, in relation to which that person is a facility holder, in these circumstances that other financial institution, having obtained the said written confirmation, is not required to verify the identity of the person.

45 The proviso to sections 8(6), 9(6), 11(3) and 11(4) of the Financial Transactions Reporting Act, 2000 provides that confirmation may be

accepted from a foreign financial institution in the circumstances set out in these sections, only if such institution is located in a country mentioned in the First Schedule to the Act. Insurance services providers should take steps to ensure that the foreign financial institution does actually exist and is contained on the relevant regulator's list of regulated institutions or by checking with a correspondent institution in the home country.

46 Section 11(5) of the Financial Transactions Reporting Act, 2000 provides that, where pursuant to any provision of Part II of that Act, a trustee, or administration manager or the investment manager of a superannuation scheme is required to verify the identity of any person because the person has become or is seeking to become a member of the superannuation scheme which is established principally for the purpose of providing retirement benefits to employees, that trustee or manager shall be deemed to have complied with the requirement to verify the identity of that person if that person's identity has been verified by his or her employer.

ACCOUNT/FACILITY OPENING FOR PERSONAL CUSTOMERS

BAHAMIAN RESIDENT PERSONAL CUSTOMERS (FACILITY HOLDERS)

47 In accordance with the Financial Transactions Reporting Regulation 2000, where a financial institution is required to verify the identity of any person, the following information is required -

(a) full and correct name of person;

(b) permanent address;

(c) telephone and fax number (if any);

(d) date and place of birth;

(e) nationality;

(f) occupation and name of employer (if self employed, the nature of the self employment);

(g) copy of relevant pages of passport, drivers licence, voter's card, national identity card or such other identification document bearing a photographic likeness of the person as is reasonably capable of establishing the identity of the person;

(h) specimen signature of the individual;

(i) purpose of the account and the potential account activity;

(j) source of funds

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

(l) such documentary or other evidence as is reasonably capable of establishing the identity of that person.

In addition to the name verification, it is important that the current permanent address should also be verified. Some of the best means of verifying addresses are:

- driver's licence;
- checking the voters Card
- making a credit reference agency search;
- requesting sight of a national insurance card, recent real property tax bill, utility bill, local authority tax bill, bank or trust company's statement (to guard against forged or counterfeit documents care should be taken to check that the documents offered are originals);
- checking a local telephone directory.

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

Because documents providing photographic evidence of identity need to be compared with the applicant's appearance, and to guard against dangers of postal intercept and fraud, prospective customers should not be asked to send these identity documents by post to a financial institution.

As far as reasonably practicable, it is expected that all documentation regarding verification of identity be current.

OPENING ACCOUNTS/FACILITIES BY POST, TELEPHONE OR INTERNET

48 Any account, which is opened without face-to-face contact between financial institutions and customers, inevitably poses difficulties for customer identification. Particular care should be taken when dealing with applications for accounts which are opened by post, telephone, internet or other electronic means, including for example requesting certified copies of documents, to ensure that personal verification and the guidance given in paragraph 47 above for verification of identity has been followed.

OPENING ACCOUNT/FACILITIES FOR STUDENTS AND YOUNG PEOPLE

49 When opening accounts for students or other young persons, the normal identification procedures set out in 47 above should be followed as far as possible. Where such procedures would not be relevant, or do not provide satisfactory evidence of identity, verification could be obtained via the home address of the parent(s) or by enquiries of the college or university.

CONFIRMATION OF IDENTITY BY FINANCIAL INSTITUTIONS

50 The primary duty to verify identity using the best evidence and means available rests with the account opening institution. However, it is recognised that in some cases, and as a last resort, a financial institution may not be satisfied with the documentary evidence acquired or the results of the enquiries set out in paragraph 47.

51 In such exceptional circumstances, a financial institution may need to approach another financial institution, on a non-competitive basis, specifically for the purpose of verifying identity. In these exceptional circumstances the standard format set out in Appendix D should be used for making the enquiry.

52 To enable financial institutions to comply with the legislative requirements, it is important that all such institutions respond to such requests to verify identity positively and without undue delay.

ACCOUNT/FACILITY OPENING PROCEDURES FOR NON-BAHAMIAN RESIDENT PERSONAL CUSTOMERS

53 For prospective customers who are not normally resident in The Bahamas but who wish to access a Bahamian based insurance service or product, it is important that verification procedures similar to those for Bahamian resident customers be carried out and the same information obtained.

54 For those prospective non-Bahamian resident customers who do not make face-to-face contact, it is recognised that verification procedures

may be difficult. Copy of the relevant pages of passport, driver's licence, voter's card, national identity card or such other identification document bearing a photographic likeness of the person as is reasonably capable of establishing the identity of the person must be retained. It is impractical to set out detailed descriptions of the various identity cards and passports that might be offered as evidence of identity by foreign nationals. However, financial institutions are strongly encouraged to independently verify identity with a reputable financial institution in the applicant's country of residence.

55 For prospective non-resident customers who wish to apply for insurance services and products by post, independent verification of identity may be sought from a reputable financial institution in the applicant's country of residence. Verification details should be requested covering true name or names used, current permanent address and verification of signature.

ACCOUNT/FACILITY OPENING FOR CLUBS, SOCIETIES AND CHARITIES

56 In the case of clubs, societies and charities who apply for insurance products and services, a financial institution should satisfy itself as to the legitimate purpose of the organisation by, for example, requesting sight of the constitution, or certificate of incorporation or memorandum and articles of association. The identity of all signatories to the account should be verified initially and, when signatories change, care should be taken to ensure that the identity of each new signatory has been verified.

UNINCORPORATED BUSINESSES

57 In the case of partnerships and other unincorporated businesses whose partners/controllers have not previously been verified by the financial institution, the identity of all partners/controllers and signatories to the account should be verified in line with the requirements for personal customers set out in regulations 3 and 5 of the Financial Transactions Reporting Regulations, 2000.

58 In cases where a formal partnership arrangement exists, a mandate from the partnership authorising the opening of an account and conferring authority on those who will operate it should be obtained.

TRUST NOMINEE AND FIDUCIARY ACCOUNTS

[See also paragraphs 68-69 - "Client Accounts" Opened by Intermediaries]

59 Trust, nominee and fiduciary accounts are a popular vehicle for criminals wishing to avoid the identification procedures and mask the origin of the criminal money they wish to launder. Particular care needs to be exercised when the accounts are set up in locations with

strict bank secrecy or confidentiality rules. Trusts created in jurisdictions not listed in the First Schedule of The Financial Transactions Reporting Act, 2000 (see Appendix E) will warrant additional enquiries.

60 Verification of the identity of the settlor and any underlying beneficiary under a trust where there lies a vested interest, is required by the Financial Transactions Reporting Act, 2000. Such verification must be carried out by the financial institution providing the facility unless the transaction is or has been conducted by another financial institution (as defined in section 2(3) of the Act) on behalf of the settlor and beneficiary and such financial institution is itself required to verify the identity of the settlor and beneficiary. The trustees/nominees should therefore be asked to state from the outset the capacity in which they are operating or making the application. Sight of certified extracts from the original trust deed, covering the appointment and powers of the transfers or, the original trust deed itself, and any subsidiary deed evidencing the appointment of current trustee, should also be obtained. Any application to become a facility holder or undertake a transaction on behalf of another, without the applicant identifying their trust or nominee capacity, should be regarded as suspicious and should lead to further enquiries.

61 An important factor to avoid laundering via trust, nominee and fiduciary accounts is that information on the identity of the settlor and/or beneficial owner of the funds, who provide the funds, and of any controller or similar person having power to appoint or remove the trustees or fund managers and the nature and purpose of the trust must be available to law enforcement, the Financial Intelligence Unit or relevant agencies in the event of an enquiry. Financial institutions should verify the true identity of the underlying principals (the person on whose behalf a transaction, other than an occasional transaction involving more than $10,000.00 is conducted) and should also obtain written confirmation from the trustees/managers of the trust that there are no anonymous principals.

PERSONAL TRUSTEES AND NOMINEES

62 Where the financial institution has not previously verified the identity of a trustee or has no current relationship with a trustee, verification of the identity of the trustee (or where there are several trustees, the identity of all the trustees) should be undertaken in line with the normal procedures as set out in regulation 3 of the Financial Transactions Reporting Regulations, 2000.

63 Under normal circumstances, a minor would be introduced to the financial institution by a family member or guardian who has an existing relationship with the institution concerned. In cases where a

nominee opening the account on behalf of another whose identity has not been previously identified by the financial institution, the identity of that nominee or any other person who will have control of the account must be verified.

64 For accounts opened through a school related scheme, the identity of the pupils should be verified in line with the normal procedures set out in regulation 3 of the Financial Transactions Reporting Regulations, 2000.

BAHAMIAN OR OVERSEAS INTERMEDIARIES ACTING AS TRUSTEES

65 Where a person who makes a request to become a facility holder or to undertake a transaction is a professional adviser, business or company acting as trustee or nominee in relation to a third party, the financial institution should verify the identity of the trustee, nominee or fiduciary and the nature of their trustee or nominee capacity or duties. Enquiries should be made by reference to appropriate, independent professional advisors as to the identity of all parties for whom the trustee or nominee is acting and confirmation sought that the source of funds or assets under the trustee's control can be vouched for. The result of the enquiries should be recorded on the account opening file.

66 Measures to obtain the information concerning the underlying beneficiary will need to take account of legal constraints and/or good market practice in the respective area of activity, the geographical location of the trustees and beneficiaries to which the trust account relates and, in particular, whether it is normal practice in those areas or markets to operate on behalf of undisclosed principals. Trusts created in poorly regulated jurisdictions may warrant additional enquiries.

67 Where money is received by a trust, it is important to ensure that the source of the funds is properly identified, the nature of the transaction is understood, and payments are made only in accordance with the terms of the trust and are properly authorised in writing.

"CLIENT ACCOUNTS" OPENED BY INTERMEDIARIES

68 Insurance brokers, stockbrokers, fund managers, attorneys, accountants, real estate brokers and other intermediaries frequently hold funds on behalf of their clients in "client accounts" opened with financial institutions. Such accounts may be general omnibus accounts holding the funds of many clients or they may be opened specifically for a single client.

69 The Financial Transactions Reporting Act, 2000 require the financial institution not only to verify the identity of the intermediary but also to look through him to his underlying clients except in the following cases:

i. the intermediary is itself a Bahamian financial institution as set out in section 2(3) of the Financial Transactions Reporting Act, 2000.

ii. the intermediary is a bank or trust company, a life assurance company, a licensed casino operator or broker-dealer, or a mutual fund administrator or operator in a country listed in the First Schedule of the Financial Transactions Reporting Act, 2000 and confirmation in writing is obtained from such an institution that it has verified the identity of the underlying clients.

Where the intermediary is not a financial institution as set out in subparagraph 8(i) and (ii) and is from a country that is not listed in the First Schedule to the Financial Transactions Reporting Act, 2000, measures must be taken to verify the identity of the underlying client. In satisfying this requirement, the financial institution should have regard to the nature of the intermediary and their degree of confidence in it, to its geographical base and to the type of business being done.

ACCOUNT/FACILITY OPENING FOR CORPORATE CUSTOMERS

70 Because of the possible difficulties of identifying beneficial ownership, and the complexity of their organisations and structures, corporate and legal entities are the most likely vehicles for money laundering, particularly when fronted by a legitimate trading company. Particular care should be taken to verify the legal existence of the applicant (i.e., the company) and to ensure that any person purporting to act on behalf of the applicant is fully authorised. The principal requirement is to look behind the corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention paid to any shareholders or others who inject a significant proportion of the capital or financial support. Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose and that it is not merely a 'shell company' where the controlling principals cannot be identified.

71 Before a business relationship is established, measures should be taken by way of a company search and/or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, struck off, wound-up or terminated.

72 As with personal accounts, the 'know your customer' principle requires an on-going process. If changes to the company structure or ownership occur subsequently, or if suspicions are aroused by a change in the

nature of the business transacted or the profile of payments through a company account, further checks should be made to ascertain the reason for the changes.

BAHAMIAN REGISTERED COMPANIES

73 The following documents are required in accordance with regulation 4 of the Financial Transactions Reporting Regulations, 2000:

(a) certified copy of the certificate of incorporation;

(b) certified copy of the Memorandum and Articles of Association of the entity;

(c) location of the registered office or registered agent of the corporate entity;

(d) resolution of the Board of Directors authorizing the opening of the account and conferring authority on the person who will operate the account;

(e) confirmation that the corporate entity has not been struck off the register or is not in the process of being wound up, e.g. certificate of good standing;

(f) names and addresses of all officers and directors of the corporate entity;

(g) names and addresses of the beneficial owners of the corporate entity;

(h) description and nature of the business including:

(i) date of commencement of business;

(ii) products or services provided;

(iii) location of principal business;

(i) purpose of the account and the potential parameters of the account including –

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

(ii) balance ranges, in the case of deposit accounts;

(iii) the expected transaction volume of the account;

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

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

In addition, a search of the file at the Companies Registry or an enquiry via a business information service or an undertaking from a firm of lawyers or accountants confirming the documents submitted to the Registrar of Companies may be made.

74 In the case of a Bahamian private company the identity of all persons authorised to operate the account should be verified in line with the requirements as contained by regulation 3 of the Financial Transactions Reporting Regulations, 2000. When signatories to the account change, care should be taken to ensure that the identities of all signatories have been verified.

75 In addition, periodic enquiries may be made to establish whether there have been any changes to the original nature of the business/activity. Such changes could be significant in relation to potential money laundering activity even though authorised signatories have not changed.

NON-BAHAMIAN REGISTERED COMPANIES

76 For non-Bahamian registered companies, the financial institution may seek to identify the directors and influential shareholders of the company in accordance with the requirements for non-Bahamian personal customers. These steps must extend as far as practicable to identifying those who ultimately own and control the company. Evidence that the individual representing the company has the necessary authority to do so should be sought and retained.

77 Comparable documents as are required for Bahamian corporate customers must be obtained. If the company is already in existence when the account in this country is opened, the signatures on the mandate must be authenticated by the company's current overseas bankers.

78 However, standards of control vary between different countries and attention should be paid to the place of origin of the documents and the background against which they are produced.

TAKING OF WHOLESALE FOREIGN CURRENCY DEPOSITS

79 For non-Bahamian registered companies, the licencee may seek to identify the officers, directors and shareholders of the company in accordance with the requirements for non-Bahamian personal customers. These steps must extend as far as practicable to identifying those who ultimately own and control the company. Evidence that the individual representing the company has the necessary authority to do so should be sought and retained.

80 Comparable documents as are required for Bahamian corporate customers must be obtained. If the company is already in existence when the account in this country is opened, the signatures on the mandate must be authenticated by the company's current overseas bankers.

81 However, standards of control vary between different countries and attention should be paid to the place of origin of the documents and the background against which they are produced.

VERIFICATION OF OTHER REGULATED FINANCIAL INSTITUTIONS

82 For financial institutions regulated by countries other than those listed in the First Schedule of the Financial Transaction Reporting Act, 2000 it is recommended that the confirmation of the existence of a financial institution and its regulated status be checked by the following means:

- checking with the home country's insurance regulator;
- checking with another office, subsidiary, branch in the same country;
- obtaining from the relevant institution evidence of its licence or authorisation to conduct the business of insurance service providers.

83 Information on insurance service providers worldwide can be obtained from any of the major international business information services.

84 Other unregulated financial institutions, should be verified in accordance with the procedures for other non-financial companies and businesses.

THE ROLE OF OTHER BROKERS

85 Where business is introduced by a correspondent broker, the financial institution is required to verify the identity of the broker and the ultimate counterparty in accordance with the Financial Transactions Reporting Regulations, 2000.

V - RECORD KEEPING

86 Sections 23, 24 and 25 of the Financial Transactions Reporting Act, 2000 require financial institutions to retain records concerning customer identification and transactions for use as evidence in any investigation into money laundering. This is an essential constituent of the audit trail procedures that the Financial Transactions Reports Regulations, 2000, seek to establish. If the Financial Intelligence Unit and law enforcement agencies investigating a money laundering case cannot link criminal funds passing through the financial system with the original criminal money, generating such funds, then confiscation of the criminal funds cannot be effected.

87 Often the only valid role a financial institution can play in a money laundering investigation is through the provision of relevant records, particularly where the money launderer has used a complex web of transactions specifically for the purpose of confusing the audit trial.

88 The records prepared and maintained by any financial institution on its customer relationships and transactions should be such that:

- requirements of legislation are fully met;
- competent third parties will be able to assess the institution's observance of money laundering policies and procedures;
- any transactions effected via the institution can be reconstructed; and,
- the institution can satisfy within a reasonable time any enquiries or court orders from the appropriate authorities.

89 The most important single feature of the Financial Transaction Reporting Act, 2000 in relation to record keeping is that it requires relevant records to be retained for at least five years from the date a person ceases to be a facility holder or from the date of completion of a transaction.

DOCUMENTS VERIFYING EVIDENCE OF IDENTITY

90 Section 24 of the Financial Transactions Reporting Act, 2000 provides that where a financial institution is required by section 6, 7, 8, 9, or 11 of the Financial Transactions Reporting Act, 2000 to verify the identity of any person, the financial institution must keep such records as are reasonably necessary to enable the nature of the evidence used for the purposes of that verification to be readily identified by the Financial Intelligence Unit.

The obligation to retain records also applies where a financial institution verifies the identity of any person by confirming the existence of a facility provided by another financial institution. In this instance, the records that are retained should be such as are

reasonably necessary to enable the Financial Intelligence Unit to readily identify, at any time, the other financial institution, the relevant facility and to confirm that the other financial institution has verified the person's identity.

Records relating to the verification of the identity of persons making a request to become facility holders, and to the identity of existing facility holders must be retained for five years after a person or financial institution ceases to be a facility holder.

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

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

91 Section IV of these Guidelines sets out the nature of the evidence to be obtained.

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

(i) the carrying out of a one-off transaction or the last in the series of transactions; or,

(ii) the ending of the business relationship, i.e., the closing of the account or accounts; or,

(iii) the commencement of proceedings to recover debts payable on insolvency.

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

93 The objective of the statutory requirements detailed in the preceding paragraphs is to ensure, in so far as is practicable, that in any subsequent investigation the financial institution can provide the authorities with its section of the audit trail. These record keeping requirements are separate from those of the regulator, but there is a considerable degree of overlap.

94 The investigating authorities need to be able to compile a satisfactory audit trail for suspected laundered money and to be able to establish a

financial profile of any suspect account. For example, the following information may be sought as part of an investigation into money laundering:

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

(ii) the volume of funds flowing through the account; and for selected transactions:

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

95 Section 28(3) of the Financial Transactions Reporting Act, 2000 provides that where the records relate to on-going investigations, they must be retained until it is confirmed that the case has been closed.

FORMAT OF RECORDS

96 It is recognised that financial institutions will find it necessary to rationalise their hard copy filing requirements. Most will have standard procedures which seek to reduce the volume and density of records which have to be stored, whilst still complying with statutory requirements. Retention may, therefore, be by way of original documents, stored on microfiche, computer disk or in other electronic form (see regulation 11 of the Financial Transactions Reporting Regulations, 2000).

AUTHENTICATION OF COMPUTERISED RECORDS

97 For computerised evidence to be admissible in a court of law, a certification confirming the computer's reliability is required pursuant to section 61 of the Evidence Act, 1996.

MICROFILM COPIES OF DOCUMENTS

98 Section 177 of the Evidence Act, 1996 also deals with the production of evidence of records in written form as well as those kept on microfilm, magnetic tape or any other form of mechanical or electronic data retrieval mechanism.

WIRE TRANSFER TRANSACTIONS

99 Investigations of major money laundering cases internationally over the last few years have shown that criminals make extensive use of electronic payment and message systems. The rapid movement of funds between accounts in different jurisdictions increases the complexity of investigations. In addition, investigations become even more difficult to pursue if the identity of the original ordering customer or the ultimate beneficiary is not clearly shown in an electronic payment message instruction.

100 In an effort to ensure that the SWIFT system is not used by criminals as a means to break the money laundering audit trail, SWIFT, at the request of the Financial Action Task Force, has asked all users of its system to ensure that when sending SWIFT MT 100 messages (customer transfers), the fields for the ordering and beneficiary customers should be completed with their respective names and addresses.

101 Subject to any technical limitations, ordering customers should be encouraged to include this information for all credit transfers made by electronic means, both domestic and international, regardless of the payment or message system used. In cases where this is not contained in the message, full records of the ordering customer and address must be retained by the originating financial institution. The records of electronic payments and messages must be treated in the same way as any other records in support of entries in the account and kept for a minimum of five years.

VI - RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

RECOGNITION OF SUSPICIOUS TRANSACTIONS

102 As the types of transactions which may be used by a money launderer 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 recognise 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

103 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

104 There is a statutory obligation on all employees to report suspicions of money laundering to the "appropriate person". For the purposes of these Guidelines, the "appropriate person" is identified and appointed as the Money Laundering Reporting Officer (MLRO or Compliance Officer) in accordance with regulations of the Financial Transactions Reporting Regulations, 2000. Once an employee has reported his or her suspicion to the MLRO or Compliance Officer, he or she has fully satisfied the statutory obligation.

All financial institutions have an obligation to ensure-

- that all prospective suspicious transactions will be passed without delay to the Money Laundering Reporting Officer or Compliance Officer; and
- that the Money Laundering Reporting Officer or Compliance Officer should be resident in The Bahamas in order to facilitate expeditions reporting of all suspicious transactions to The Financial Intelligence Unit.

THE ROLE OF THE MONEY LAUNDERING REPORTING OFFICER

106 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, but he or she should be sufficiently senior to command the necessary authority. Larger financial institutions may choose to appoint a senior member of their compliance, internal audit or fraud departments. In small organisations, 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.

107 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.

108 In making this judgment, he or she should consider all other relevant information available within the financial institution concerning the person or business 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, then he or she must disclose this information to the Financial Intelligence Unit.

109 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 he or she must give his reasons for negating, and therefore not reporting any particular matter, but it clearly would be prudent, for his or her own protection, for internal procedures to require that only written reports are submitted to him or her and that he or she should record his or her determination in writing.

110 The Money Laundering Reporting Officer will be expected to act honestly and reasonably and to make his or her determinations in good faith.

REPORTING PROCEDURES

111 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.

112 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, and in cases of urgency, reports may be made orally.

113 Sufficient information should be disclosed which indicates the nature of and reason for the suspicion. Where the financial institution has

additional relevant evidence that could be made available, the nature of this evidence should also be clearly indicated.

Pursuant to section 14(2) of the Financial Transactions Reporting Act, 2000, persons submitting suspicious transactions reports are required to provide the relevant information to The Financial Intelligence Unit in the form attached as Appendix G of these Guidelines.

114 The receipt of a disclosure will be acknowledged by the Financial Intelligence Unit. Normally, completion of a transaction or the 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 financial institution will be required to discontinue the transaction or cease operation of the customer's account.

115 Following receipt of a disclosure and initial research by the Financial Intelligence Unit, if appropriate, the information disclosed is allocated to trained financial analysts in the Financial Intelligence Unit for further analysts. This is likely to include seeking supplementary information from the organisation making the disclosure, and from other sources. Discreet enquiries are then made to confirm the basis for suspicion. The customer is not approached in the initial stages of the analysis of a disclosure and will not be approached unless criminal conduct is identified.

116 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 and law enforcement agencies and financial institutions is considered to be of paramount importance.

117 It is recognised that the provision of information inviting the inference that a customer is suspected of involvement in criminal activity might have an influence on the commercial decisions made subsequently by the disclosing institution. The draft of the letter at Appendix H has been worded with this consideration in mind.

118 It is also recognised 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.

119 Financial institutions are reminded that reporting to entities identified in section 18 of the Financial Transactions Reporting Act, 2000 (see Summary) 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 the 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 (see summary of legislation in Appendix B).

120 Following the submission of a disclosure report, a financial institution is not precluded from subsequently terminating its relationship with the customer provided it does so for commercial or risk containment reasons and does not alert the customer to the fact of the disclosure which would constitute the offence of tipping off pursuant to section 20(5) Financial Transactions Reporting Act, 2000. However, it is recommended that before terminating a relationship in these circumstances, the reporting institution should liaise directly with the relevant officer in the Financial Intelligence Unit to ensure that the termination does not tip off the customer or prejudice the investigation in any other way.

FEEDBACK FROM THE INVESTIGATING AUTHORITIES

121 The provision of feedback by the Financial Intelligence Unit to the financial institution by whom suspicions are reported is recognised as an important element of the system which has been developed. The provision of general feedback to the financial sector on the volume and quality of disclosures and on the levels of successful investigations arising from the disclosures will be provided on a regular basis through the Financial Intelligence Unit.

122 Financial institutions should ensure that all contact between their departments or branches, with the Financial Intelligence Unit and law enforcement agencies is reported to the Money Laundering Reporting Officer so that an informed overview of the situation can be maintained. In addition, the Financial Intelligence Unit will continue to provide information on request to a disclosing institution in order to establish the current status of a specific investigation.

VII - EDUCATION AND TRAINING

REQUIREMENTS

123 Financial institutions must take appropriate measures to make employees aware of:

- policies and procedures put in place to detect and prevent money laundering including those for identification, record keeping and internal reporting; and

- the relevant legislation pertaining to money laundering;

and to provide relevant employees with training in the recognition and handling of suspicious transactions.

124 These Guidelines therefore set out what steps financial institutions should take to fulfill this requirement.

THE NEED FOR STAFF AWARENESS

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

126 It is, therefore, important that organisations conducting insurance business as defined by the Insurance Act, Chapter 317, and the External Insurance Act, Chapter 318 respectively covered by these Guidelines introduce comprehensive measures to ensure that staff are fully aware of their responsibilities.

EDUCATION AND TRAINING PROGRAMMES

127 Timing and content of training for various sectors of staff will need to be adapted by individual institutions for their own needs. The Financial Intelligence (Transactions Reporting) Regulations, 2000 provide that, at least once per year, financial institutions shall provide relevant

employees with appropriate training in the recognition and handling of suspicious transactions. The following is recommended:

(a) New Employees

A general appreciation of the background to money laundering, and the subsequent need for reporting of any suspicious transactions to the Money Laundering Reporting Officer should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority, within the first month of their employment. They should be made aware of the importance placed on the reporting of suspicions by the organisation, that there is a legal requirement to report, and that there is a personal statutory obligation in this respect. They should also be provided with a copy of the written policies and procedures in place in the financial institution for the reporting of suspicious transactions.

(b) Front Line Staff

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

(c) Account/Facility Opening Personnel

Those members of staff responsible for account opening and acceptance of new customers must receive the basic training given to front line staff in the above paragraph. In addition, further training should be provided in respect of the need to verify a customer's identity and on the business' own account opening and customer/client verification procedures. They should also be familiarised with the business' suspicious transaction reporting procedures.

(d) Administration/Operations Supervisors and Managers

A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising from the Proceeds of Crime Act, 2000 and the Financial Transactions Reporting Act, 2000 for non-reporting and for assisting money launderers; procedures relating to the service of production and restraint orders; internal reporting procedures and the requirements for verification of identity, the retention of records, and disclosure of suspicious transaction reports under the Financial Intelligence Unit Act, 2000.

(e) Money Laundering Reporting Officer/Compliance Officer

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

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

****

APPENDIX A

MONEY LAUNDERING SCHEMES UNCOVERED

Account Opening with Drafts

1. 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 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

2. 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 sales 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.

3. 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

4. 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

5. A fraud investigation into the collapse of a wholesale supply company revealed 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

6. 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 organised 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 fourteen 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

7. 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

8. 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

9. 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

10. 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

11. **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 cashiers 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 in the U.S. 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

12. **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 air freight. 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 both for fraud prevention and for 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'

13. **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

14. **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 law 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 drug trafficker's funds were confiscated by the Court, 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

15. **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, 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 nine 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 and then put down £45,000.00 deposit on a new one, had a £6,700.00 holiday in Seychelles, bought a Land Rover Discovery, and made 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 is 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

16. **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 the 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 traveller 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, 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 of an 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 institution discuss their situation with the senior officer of the Financial Investigation Unit team in order to agree the course of action.

APPENDIX B

SUMMARY OF EXISTING BAHAMIAN LAW

The existing law pertaining to money laundering and the requirements that financial institutions know their customers are found substantially in the Proceeds of Crime Act, 2000 (Act No. 44 of 2000), the Financial Transactions Reporting Act, 2000 (Act No. 40 of 2000), the Financial Transactions Reporting (Amendment) Act, 2001 (Act No. 17 of 2001), the Financial Transactions Reporting Regulations, 2000 (Statutory Instrument No. 111 of 2000), the Financial Transactions Reporting (Amendment) Regulations, 2001 (Statutory Instrument No. 113 of 2001), the Financial Intelligence Unit Act, 2000 (Act No. 39 of 2000), the Financial Intelligence Unit (Amendment) Act, 2001 (Act No. 20 of 2001) and the Financial Intelligence Unit (Transactions Reporting) Regulations, 2001 (Statutory Instrument No. 7 of 2001).

I PROCEEDS OF CRIME ACT, 2000

Confiscation Orders

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

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

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

(1) An offence under the Prevention of Bribery Act, Chapter 81;

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

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

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

The court must first determine whether such a person has benefited from the principal offence or offences for which he is to be sentenced and secondly from

any relevant offences which the court will be taking into consideration in determining his sentence for the principal offence.

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

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

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

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

(a) that any property shown to the court

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

(ii) to have been transferred to him at any time since the beginning of the period of six years ending when the proceeding was instituted against him,

was received by him as a payment or reward in connection with drug trafficking carried on by him;

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

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

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

Charging Orders

Section 27 of the Act provides that a court may make a charging order imposing a charge on property specified in the order for securing the payment of

money to the Crown. An application for a charging order may be made only by the Police or the Attorney-General. Property which may be the subject of a charging order includes, inter alia, any monies held by or deposited with a bank or other financial institution, stock of any body corporate, and a debt instrument.

Production Orders

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

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

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

Monitoring Order

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

The monitoring order is to be made where the Judge is satisfied by evidence on oath that there is reasonable cause to believe that a person has committed or is about to commit a drug trafficking offence or a relevant offence; or was involved in the commission or is about to become involved in the commission of such an offence; or has benefited directly or indirectly from the commission of such an offence. The disclosure of information in these circumstances is not to be treated as a breach of any restriction upon disclosure of information imposed by the Banks and Trust Companies Regulation Act, 2000, The Central Bank of The Bahamas Act, 2000, any other statute or otherwise. Additionally, such disclosure shall not give rise to any civil liability.

The Offence of Money Laundering

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

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

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

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

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

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

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

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

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

It is a defence for a person to prove that he acquired or used the property or had possession of it for adequate consideration.

Penalty for failing to disclose suspicious transaction

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

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

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

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

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

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

Penalty for offences under sections 43 and 44

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

Penalty for Money Laundering

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

External Confiscation Orders

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

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

Offences by a body corporate

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

II. THE FINANCIAL TRANSACTIONS REPORTING ACT, 2000

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

Section 2(3) of the Act restricts the definition of "financial institution" to include only five of the institutions listed in section 3 of the Act, namely banks or trust companies, companies carrying on life assurance business, licensed casino operators, and mutual fund administrators or operators of mutual funds (see sections 3(1)(a), (b), (e), (f) and (i)). For the purposes of section 7(2)(b), 8(6)(c), 9(6)(c), 11(3)(b)(iii) and 11(4)(b)(iii) of this Act institutions referred to section 2(3) may obtain written confirmation from other financial institutions listed in section 2(3), for the purpose of verifying a customer's identity.

NB: The occasions when a financial institution may obtain and rely upon written confirmation of identity from another such institution are set out in Part IV of these Guidelines in paragraphs 32-45, above.

Section 3 of the Act, defines "Financial Institution".

The Financial Transactions Reporting Act, 2000 makes it mandatory for financial institutions to verify the identity of the following persons:

Section 6 - Persons who wish to become facility holders

The identity of such persons must be verified before they become facility holders (see section 6(1) and 6(2)).

Each and every existing facility holder.

The identity of these persons must be verified within twelve months from the date of the commencement of this Act, or within twenty-four months from the commencement of this Act if so ordered by the Minister.

Where at the end of the twelve months or, as the case may be, the twenty-four month period, the financial institution is unable to verify the identity of the facility holder, the financial institution shall assign the facility to the Central Bank of The Bahamas in accordance with section 16 of the Banks and Trust Companies Regulation Act, 2000 (see section 6(6)).

Existing facility holders whose identities are doubtful.

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

Occasional Transactions

Section 7 of the Act provides (subject to certain exceptions) for the mandatory verification by a financial institution of the identity of the following persons:

A person who conducts an occasional transaction by, through or with a financial institution in any case where:

(a) the amount of cash involved in the transaction exceed the prescribed amount of $10,000.00, (this verification must take place before the transaction is conducted) and in these circumstances, the financial institution shall also ask the person who is conducting or who has conducted the transaction whether or not the transaction is or was being conducted on behalf of any other person; or,

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

(c) the financial institution has reasonable grounds to believe that the transactions have been or are being structured so that the amount of cash involved in the transaction do not exceed the prescribed amount of $10,000.00; and

(d) the total amount of funds involved in those transactions exceeds the prescribed amount.

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

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

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

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

Section 8 of the Act provides (subject to certain exceptions) for the mandatory verification by a financial institution of the identity of the following persons:

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

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

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

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

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

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

Section 9 of the Act provides (subject to certain exceptions) for the mandatory verification of the identity of the persons on whose behalf a transaction is being or has been conducted by a facility holder in relation to and through a facility provided by a financial institution where:

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

  (a) the amount of cash involved in the transaction exceeds the prescribed amount of $10,000.00; and,

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

  Such verification must take place before the transaction is conducted.

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

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

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

  Such verification must take place as soon as practicable after these conditions are satisfied.

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

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

Such verification may be accepted from a foreign financial institution if that institution is located in a country mentioned in the First Schedule.

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

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

(b) in contravention of section 7(4)(a), permits any person to conduct an occasional transaction in excess of $10,000.00 without first having verified the identity of that person;

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

(d) in contravention of section 8(4) fails to verify the identity of a person on whose behalf an occasional transaction in excess of $10,000.00 is being or has been conducted;

(e) in contravention of section 8(5), fails to undertake the verification required by section 8(2) in relation to persons conducting an occasional transaction in excess of 10,000.00 in circumstances where it reasonably appears that the transaction is being conducted on behalf of any other person or persons and that the transactions are or have been structured to avoid verification of identity;

(f) in contravention of section 9(4), fails, before a transaction is conducted, to verify the identity of a person on whose behalf a facility holder is conducting a transaction in excess of $10,000.00 where it has reasonable grounds to believe that the circumstances set out in section 9(1) exist, and;

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

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

(a) in the case of an individual, $20,000.00;

(b) in the case of a body corporate, $100,000.00.

Suspicious Transactions

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

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

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

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

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

Oral Reports

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

Penalty for failing to report suspicious transactions

A person who contravenes the provisions of Section 14 shall be liable on summary conviction to a fine not exceeding – in the case of individuals, $20,000.00 and, in the case of a body corporate, $100,000.00

Defence

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

Auditors to report suspicious transactions

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

Protection of persons reporting suspicious transactions

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

Legal Professional Privilege

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

Persons to whom suspicious transaction reports may be disclosed

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

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

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

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

Protection of Identity

Section 19 of the Act provides that no person shall be required to disclose, in any judicial proceeding, any suspicious transaction report, or any information the disclosure of which will identify, or is reasonably likely to identify, any person as a person who, in his or her capacity as an officer, employee or agent of a financial institution, has handled a transaction in respect of which a suspicious transaction report was made as a person who has prepared a suspicious transaction report, or as a person who has made a suspicious transaction report, unless the Judge or, as the case requires, the person presiding at the proceeding is satisfied that the disclosure of the information is necessary in the interests of justice.

Penalty for Making False Statements and for wrongful disclosure

Section 20 of the Act provides that:

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

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

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

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

(2) either:

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

b. with intent to prejudice any investigation into the commission or possible commission of a money laundering offence;

discloses that information to any other person is guilty of an offence (see section 20(5)).

Penalty

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

Application of information contained in a suspicious transaction report

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

Retention of Records

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

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

Section 24 of the Act provides that where a financial institution is required by section 6, 7, 8, 9, or 11 of the Act, to verify the identity of any person, the financial institution must keep such records as are reasonably necessary to enable the nature of the evidence used for the purposes of that verification to be readily identified by the Financial Intelligence Unit.

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

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

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

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

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

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

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

Section 27 of the Act provides that a company need not retain records where a company has been liquidated and finally dissolved; or, where a partnership has been dissolved.

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

Destruction of records is not required where there is a lawful reason for retaining them.

There is a lawful reason for retaining a record if the retention of a record is necessary:

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

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

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

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

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

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

III. FINANCIAL TRANSACTIONS REPORTING REGULATIONS, 2000

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

Regulation 2 provides that for the purposes of Part II of the Financial Transactions Reporting Act 2000, the prescribed amount shall be the sum of $10,000.00.

Regulation 3 sets out the information required in the case of any person and includes information such as the full and correct name of the person, their permanent address, telephone and fax numbers(if any), date and place of birth, nationality, occupation and name of employer (if self employed, the nature of the self employment), copy of the relevant pages of passport, drivers licence, voter's card, national identity card or such other identification doucment bearing a photographic likeness of the person as is reasonably capable of establishing the identity of the person.

Regulation 4 sets out the information required in the case of a corporate entity, whether incorporated in The Bahamas or elsewhere. The information required includes certified copies of the certificate of incorporation, the Memorandum and Articles of Association, the location of the registered office or the registered agent of the entity, resolution of the Board of Directors authorizing the opening of the account and conferring authority on the person who will operate the account and the names and addresses of the beneficial owners of the entity.

Regulation 5 sets out the information required for the verification of the identity of partnerships or other unincorporated businesses.

Regulation 5A provides for exemptions from verification procedures by certain financial institutions and other agencies or bodies. In particular, an applicant for insurance –

i) consisting of a policy of insurance in connection with a pension scheme taken out by virtue of a person's contract of employment;

ii) in respect of which a premium is payable in one instalment of an amount not exceeding $2,500.00; and

iii) in respect of which a periodic premium is payable and where the total payable in respect of any calender year does not exceed $2,500.00.

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

Regulation 9 provides that once verification of identity of a facility holder has been completed, no further verification of identity is necessary as long as the facility is used by the facility holder in a regular basis. Financial institutions are required to regularly monitor facility holders for consistency with the facility holder's stated account purposes and business and the identified potential account activity during the first year of operation of the facility.

Where there has been no recent contact with the facility holder or no transaction involving the facility within a period of five years, the financial institution shall verify the identity of the facility holder.

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

Regulation 11 provides that records required by section 22, 24 or 25 of the Act to be kept by any financial institution may be stored on microfiche, computer disk or in other electronic form.

IV. FINANCIAL INTELLIGENCE UNIT ACT, 2000

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

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

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

- receve all disclosures of information required to be made pursuant to the Proceeds of Crime Act, 2000;

- receive information from any foreign Financial Intelligence Unit;

- order in writing any person to refrain from completing any transaction up to a maximum period of seventy-two hours;

- freeze a person's bank account for a maximum period of 5 days upon receipt of a request from a foreign FIU or law enforcement authority including the Commissioner of Police of The Bahamas;

- require the production of information (except information subject to legal professional privilege) which it considers relevant to fulfill its functions;

- share information relating to the commission of an offence under the Proceeds of Crime Act, 2000 with the local law enforcement agency including the Commissioner of Police;

- provide information to foreign FIU's relating to the commission of an offence under the Proceeds of Crime Act, 2000;

- enter into any agreement or arrangement in writing with a foreign FIU for the discharge or performance of the functions of the FIU;

- inform the public and financial and business entities of their obligations under measures that have been or might be taken to detect, prevent and deter the commission of offences under the Proceeds of Crime Act, 2000;

- retain a record of all information it receives for a minimum of five years after the information is received

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

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

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

NO CIVIL OR CRIMINAL LIABILITY

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

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

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

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

V. FINANCIAL INTELLIGENCE (TRANSACTIONS REPORTING) REGULATIONS, 2000

The Financial Intelligence (Transactions Reporting) Regulations, 2001 require financial institution to establish and maintain the following procedures and practices:

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

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

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

The Money Laundering Reporting Officer must be registered with the FIU. Financial institutions must institute and maintain internal reporting procedures which include provisions requiring the Money Laundering Reporting Officer to disclose to the FIU, relevant agency or to a police officer the information or other matter contained in a suspicious transaction report, where

the Money Laundering Reporting Officer knows, suspects or has reasonable grounds to suspect a person is engaged in money laundering.

Regulation 6 places an obligation on financial institutions to provide appropriate training from time to time for all relevant employees, at least once per year. Financial institutions are required to take appropriate measures from time to time to make all relevant employees aware of the provisions of the Financial Intelligence Unit Act, 2000 and the Regulations made thereunder, the Financial Transactions Reporting Act, 2000, the Financial and Corporate Service Providers Act, 2000, the Proceeds of Crime Act, 2000, and any other statutory provision relating to money laudering.

Employees must also be made aware of the procedures maintained by the financial institution in complaince with the duties imposed under these regulations.

Training must be given to all new employees as soon as practicable after their appointment.

Regulation 8 provides that failure to comply with the requirements of these regulations is an offence punishable on summary conviction to a fine of $10,000.00 and; on conviction on information to a fine of $50,000.00 for a first offence; and to a fine of $100,000.00 for a second or subsequent offence.

It is a defence to prove that a financial institution took all reasonable steps and exercised due dilligence to comply with the requirements of these regulations.

In determining whether a financial institution has complied with the requirements of these regulations, the trial court shall make account of any relevant guidelines issued by the FIU or the relevant agency or both.

APPENDIX C

FINANCIAL ACTIVITIES COVERED BY GUIDELINES

Acceptance of deposits and other repayable funds from the public.

Lending/Borrowing.

Leasing.

Money transmission services (including electronic banking).

Issueing and administering means of payment (e.g., credit cards, travellers cheques and bankers drafts).

Guarantees and Commitments.

Trading for own account or for account of customers in:

(a) money market instruments ;
(b) foreign exchange;
(c) financial futures and options;
(d) exchange and interest rate instruments;
(e) transferable securities.

Participation in securities issues and the provision of services relating to such issues.

Advice to businesses on capital structure, industrial strategy and related questions and advice and services relating to mergers and the purchase of undertakings.

Money brokering.

Safekeeping and administration of securities.

Credit reference service.

Safe custody services.

Trustee services.

Portfolio management and advice.

APPENDIX D

To: From: (stamp of branch sending the letter)

Dear Sirs:

REQUEST FOR VERIFICATION OF CUSTOMER IDENTITY

In accordance with the Anti-Money Laundering Guidelines for licensed financial institutions we write to request your verification of the identity of our prospective customer detailed below.

Full name of customer .....

Title (MR/MRS/MISS/MS).....

Address including postcode .....
(as given by customer) .....

Date of birth ..... Account Number .....
(if known)

Example of customer's signature

Please respond positively and promptly by returning the tear-off portion below

.....
Authorized signature

To: The Manager (originating branch) From: (branch stamp)

Request for verification of the identity of (title and full name of customer)

With reference to your enquiry dated ..... we:

(1) Confirm that the above customer *is/is not known to us.

(2) *Confirm/cannot confirm the address shown in your enquiry.

(3) *Confirm/cannot confirm the date of birth.

(4) *Confirm/cannot confirm that the signature reproduced in your enquiry appears to be that of the above customer.

The above information is given in strict confidence, for your private use only, and without any guarantee or responsibility on the part of this financial institution or its officials.

*Delete as applicable.

.....
Authorized signature

APPENDIX E

FIRST SCHEDULE

Financial institutions as defined by section 2(3) of the Financial Transactions Reporting Act, 2000 may accept written confirmation of verification of identity from other financial institutions located in countries and territories listed below, for the purpose of sections 8(6)(c), 9(6)(c), 11(3)(b)(iii) and 11(4)(b)(iii) of the Financial Transactions Reporting Act 2000.

Australia
Barbados
Belgium
Bermuda
Brazil
Canada
Cayman Island
Channel Islands
Denmark
Finland
France
Germany
Gibraltar
Greece
Hong Kong SAR
Isle of Man
Ireland
Italy
Japan
Liechtenstein
Luxembourg
Malta
Netherlands
New Zealand
Norway
Panama
Portugal
Singapore
Spain
Sweden
Switzerland
United Kingdom
United States

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 higher denomination.

(g) Frequent exchange of cash into other 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 location 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 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 abroad.

(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 company 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 organisations.

(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 travellers cheques, foreign currency drafts or other negotiable instruments to be issued.

(g) Frequent paying in of travellers 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 direction.

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 favour, or due to the exercise of undue pressure.

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

(i) Dealing Patterns

(a) A large number of security transactions across a number of jurisdictions.

(b) 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.

(c) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual; e.g., churning at the client's request.

(d) Low grade securities purchased in an overseas jurisdiction, sold locally and high grade securities purchased with the proceeds.

(e) Bearer securities held outside a recognized custodial system.

(ii) Abnormal Transactions

(a) 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.

(b) 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.

(c) Transfer of investments to apparently unrelated third parties.

(d) 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.

(e) 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) 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.

(b) Large transaction settlement by cash.

(c) 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:

(a) Settlement to be made by way of bearer securities from outside a recognized clearing system.

(b) 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:

(a) payment to a third party without any apparent connection with the investor.

(b) settlement either by registration or delivery of securities to be made to an unverified third party.

(c) 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) client/customer 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) the customer/client 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) the customer/client 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. Insurance sector participants 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 fax or courier to the Financial Intelligence Unit,
3rd Floor, Norfolk House, Frederick Street, Nassau, Bahamas. P.O. Box SB-50086
Telephone: (242) 356-9808 or (242) 356-6327, Facsimile No.: (242) 322-5551

For Official Use Only FIU Reference Number:.....

To: **Financial Intelligence Unit – Fax: (242) 322-5551**

Date: _____ **No. of Pages:** _____

NB: Persons who report suspicious transactions are required, pursuant to section 14 of the Financial Transactions Reporting Act, 2000, to provide the Financial Intelligence Unit with the following information:

[A] Disclosing Institution

Disclosure Type:

Proceeds of Crime ☐

Drug Trafficking ☐

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] Authorised 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: .....

Assets 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

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 Managers		Internet Research	
Bureaux Des Changes		Group Information	
Stockbrokers		3rd Party Information	
Financial Advisors		Service of Production,Charging or Monitoring Order	
Insurance Companies		Service of Investigation of Fraud Order	
Trust Company		Police Enquiry	
Corporate Service Provider		Account Activity Not in Keeping with KYC	
Lawyers		Evidence of Forged Documentation	
Accountants		Cash Transactions	
Local Regulator		Transitory Accounts – Immediate Layering	
Other Regulator		High Risk Jurisdictions	
Other (specify)		Unusual Forex Transactions	
		Purchase and Surrender of Insurance Policy	
Trends?		Repeat Disclosures	
Involving at least one intermediary		Failure to comply with due diligence checks	
Long Standing Customer		Other (specify)	
New Customer			
Electronic Banking		**What currency was involved?**	
EURO Transaction		GBP	
		USD	
		EUR	
Criminality Suspected		ESP	
Drugs		GMD	
Terrorism		ITL	
Fraud		FRF	
Revenue Fraud		IEP	
Insider Dealing		SEK	
Corruption		CHF	
Unknown / Undetermined		BSD	
Regulatory Matters		OTHER	
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, Bahamas
Tel. Nos.: (242)356-9808 or (242)356-6327
Fax No.: (242322-5551

Your Ref:
Our Ref: Date:

The Manager
Financial Institution
Street Address
Nassau, Bahamas

Dear Sir:

Re: Financial Investigation Feedback Report

Following the receipt of your recent disclosure and the subsequent enquiries made by this department, I enclose for your information a summary of the present position of the case (see overleaf).

The current status shown, whilst accurate at the time of making this report, should not be treated as a basis for subsequent decision, without reviewing the up-to-date position.

Please do not hesitate to contact the undersigned at the Financial Intelligence Unit if you require any further information or assistance.

Yours faithfully,

Authorized Officer
Financial Intelligence Unit

Enclosure

RESULTS CATEGORY

☐ DRUG POSITIVE	Resulting in arrest/prosecution.
☐ DRUG SUSPECT	Related to drug trafficking without arrest/ prosecution AND/OR subject known in local indices.
☐ CRIME POSITIVE	Related to crime without arrest/prosecution AND/OR known in local indices.
☐ CRIME SUSPECT	Related to crime without arrest/prosecution AND/OR known in local indices.
☐ TERRORISM POSITIVE	Resulting in arrest/prosecution.
☐ TERRORISM SUSPECT	Resulting in arrest/prosecution.
☐ NOTED FOR INTELLIGENCE PURPOSES	Initial checks completed only, information noted for intelligence purposes.
☐ UNKNOWN	Source of funds unknown, suspicion remains unresolved.
☐ NEGATIVE	POSITIVELY established to be unconnected to crime, drug trafficking or terrorism.

Afterword

Until it is further Ordered, The Financial Intelligence Unit intends to abide by the Supreme Court decision of Her Ladyship, Justice Anita Allen in Financial Clearing Corporation v The Attorney-General No. 232 of 2001.

Please be advised that the Guidelines have not been amended to reflect the ruling of Justice Allen.