Guidelines for DNFBPs

1. Purpose

These Guidelines have been compiled by the Saint Christopher and Nevis Financial Services Regulatory Commission ("Commission") to offer guidance to Designated Non-Financial Businesses and Professions (DNFBP's) on how best to comply with Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT) applicable to their business.

These Guidelines are made pursuant to the Financial Services Regulatory Commission Act, 2009. The Guidelines represent what is considered to be best industry practice. The DNFBPs shall comply with these Guidelines

Each DNFBP is responsible for its own policies and implementation and should not rely on this publication other than as a general framework and guideline.

2. Relevant Laws

The Government of Saint Christopher and Nevis passed the following pieces of legislation in its drive to properly and effectively regulate and supervise the financial services sector and to combat money-laundering and terrorist financing.

- The Financial Services Regulatory Commission Act, 2009, (as amended)
- The Proceeds of Crime Act, 2000 (as amended) (Cap 4.28 of the 2009 Revised Laws)
- The Financial Intelligence Unit Act, 2000 (as amended) (Cap. 21.09 of the 2009 Revised Laws)
- The Anti-Money Laundering Regulations, 2011
- The Financial Services (Exchange of Information) Regulations, 2002
- The Anti-Terrorism Act, 2002 (as amended) (Cap. 4.02 of the 2009 Revised Laws)
- Anti-Terrorism (Prevention of Terrorist Financing) Regulations, 2011
- Financial Services (Implementation of Industry Standards) Regulations, 2011

3. The Financial Services Regulatory Commission Act, 2009

The Commission was established under the Financial Services Regulatory Commission Act, No. 22 of 2009 as the ultimate regulatory body for financial services, anti-money laundering and combating terrorist financing within the Federation.
The Commission is responsible, amongst its other duties, for the following:

- maintaining a general review of the operations of all regulated entities;
- monitoring financial services business carried on in or from within Saint Kitts and Nevis and for taking action against persons carrying on unauthorized business;
- monitoring compliance by regulated persons with the Proceeds of Crime Act, the Anti-Terrorism Act and such other Acts, regulations, codes or guidelines relating to money laundering or the financing of terrorism that are set out in Schedule 1;

The Commission is comprised of seven (7) members, including persons drawn from the Ministry of Finance on both islands as well as nominees from the Central Bank, the Ministry of Legal Affairs and the Financial Intelligence Unit.

SAINT CHRISTOPHER AND NEVIS FINANCIAL SERVICES REGULATORY COMMISSION

St. Christopher
The Director,
Financial Services Regulatory Commission – St. Kitts Branch
Upstairs Karibhana Building,
Liverpool Row,
P. O. Box 898,
Basseterre

Telephone: (869) 466-5048
(869) 465-2521 Ext. 1019
Facsimile: (869) 466-5317
Email: skanfsd@sisterisles.kn
Website: www.fsrc.kn

Nevis
The Director
Financial Services Regulatory and Supervisory Department
Ministry of Finance
P. O. Box 689
Main Street
Charlestown

Telephone: (869) 469-1469

(869) 469-5521 Ext 2150
Facsimile: (869) 469-7739
Email: info@nevisfsrc.com
Website: www.nevisfsrc.com

In the exercise of its functions, the Commission is guided primarily by the following principles:

- The reduction of risk to the public of financial loss due to dishonesty, incompetence or malpractice by the financial unsoundness of persons carrying on the business of financial services;

- The protection and enhancement of the reputation and integrity of the Federation in commercial and financial matters; and

- The best economic interests of the Federation.

The Commission, as the body set up under Federal law "to take such steps as the Commission considers necessary or expedient for the development and effective regulation and supervision of finance business in Saint Christopher and Nevis" and to "have regard to the protection and enhancement of the reputation and integrity of Saint Christopher and Nevis in commercial and financial matters", takes the following view:

- A critical factor in the success of our anti-money laundering and counter financing of terrorism initiatives is the establishment of a culture of compliance and due diligence throughout the entire business community, both regulated and unregulated. In order to demonstrate compliance with the 2012 revised forty recommendations of the Financial Action Task Force (FATF) in reference to money laundering and the combating of terrorist financing, the Regulators appointed by the Commission will regularly conduct a program of on-site examinations to monitor compliance of all businesses engaged in financial services with these Guidance Notes.

These Guidelines are a statement of the standard expected by the Commission of all Designated Non-Financial Businesses and Professions (DNFBP) under the Proceeds of Crime Act, 2000, the Anti-Terrorism Act, 2002 and the Financial Services Regulatory Commission Act, 2009 in the Federation of Saint Christopher and Nevis. The Commission actively encourages all DNFBPs to develop and maintain links with the Departments established under it in both Saint Christopher and Nevis to ensure that its policies, and systems of procedures and controls (vigilance systems) to guard against money laundering and terrorist financing, are effective and up to date.

4. The Financial Services (Exchange of Information) Regulations 2002

The Financial Services (Exchange of Information) Regulations, 2002 provide guidelines under which the Regulators of all businesses engaged in financial services in the Federation of Saint Christopher and Nevis have a legal obligation to co-operate with foreign regulatory authorities.

The Regulations provide for the regulatory authority of Saint Christopher and Nevis to take certain matters into consideration before it shares information or provides assistance to a foreign regulatory authority. Some of the issues that must be considered before information is shared are the nature and seriousness of the matter being investigated, public interest considerations and any agreements on sharing of information that the Federation of Saint Christopher and Nevis has with the requesting state.

The Regulations also provide for the regulatory authority to request information required by the foreign regulatory authority from the relevant regulated persons if the regulatory authority is satisfied that assistance should be provided and the information required is not in its possession. The regulatory authority must also seek a Court Order to compel the production of the information required if regulated persons or businesses do not comply with its request.
Information supplied to a foreign regulatory authority shall not be disclosed to any other person or authority by the foreign regulatory authority without the consent of the person from whom the Saint Christopher and Nevis regulatory authority obtained the information.

Persons who fail to comply with a Court Order for information to be supplied or who falsify information provided or destroy information or who disclose information contrary to the Regulations, commit an offence and are liable on summary conviction to a fine not exceeding $100,000.00 or to imprisonment for a term not exceeding two years or both.

5. The Proceeds of Crime Act 2000

The Proceeds of Crime Act, 2000 covers all serious offences.

DNFBPs are listed in the Schedule to the Act.

Under Section 65, a person who is convicted of a serious offence under the Act, shall not be eligible to or be licensed to carry on a regulated business.

Regulations

The Anti-Money Laundering Regulations, 2008 were issued in July 2008 pursuant to Section 67 of the Act. These regulations prescribe the identification, record-keeping, internal reporting and training procedures to be implemented and maintained by any person carrying on a regulated business for the purpose of forestalling and preventing money laundering. The Regulations have been revised and are now embodied in the Anti-Money Laundering Regulations 2011.

6. The Financial Intelligence Unit Act 2000

All businesses included in the Schedule to the Proceeds of Crime Act, 2000, and the Anti-Terrorism Act, 2002 including regulated businesses such as DNFBPs are required as an obligation, to develop and maintain links through their compliance officer (such officer having been approved by the Financial Services Regulatory Commission), with the Financial Intelligence Unit (FIU), which was established under the Financial Intelligence Unit Act, 2000. The Unit has been set up to receive, collect and analyze reports of suspicious transactions from financial services and other businesses which are required to be made under the Proceeds of Crime Act, 2000 and on being satisfied that there are reasonable grounds to suspect that funds are linked or related to or to be used for the purposes of a money laundering or terrorist financing offence, submit a report to the Commissioner of Police for necessary action. The Unit should, upon receipt of a report of a suspicious transaction, order any person in writing, to refrain from completing any transaction for a period not exceeding seventy-two hours.

The Unit shall require the production of information from those businesses which have made reports to it. The failure or refusal to provide such information is an offence under the Act.

The Unit is also responsible for informing 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 money laundering or terrorist financing offences.

The Act further provides for the establishment of a governing agency, known as the FIU Body. In addition to a Director, who shall be responsible for managing the day-to-day affairs of the Unit, this body is comprised of representatives from the Attorney General's Chambers, the Ministries of Finance of both islands, the Legal Department, Nevis and police officers who are qualified financial investigators.

FINANCIAL INTELLIGENCE UNIT (FIU)

The Director,
2nd Floor Ministry of Finance
Basseterre,
Saint Christopher & Nevis.
Telephone: (869) 466 3451
Facsimile: (869) 466 4945
E mail: sknfiu@thecable.net

7. The Anti-Terrorism Act, 2002

The Anti-Terrorism Act, 2002 applies to all persons including corporate bodies and covers, inter alia, the following:

- The designation of terrorist groups, the offences of: belonging to, supporting or wearing the uniform of a terrorist group.
- The offences of terrorist financing, the use of property for terrorist activity and engaging in money laundering for terrorist purposes.
- The offences of participating in terrorist activities, training of terrorists, possession of articles for terrorist purposes and inciting terrorism abroad.
- The power of the authorities to freeze property related to terrorist activity or the property of a person convicted of a terrorist offence;
- Investigative powers that should be used by the police in the investigation of terrorist offences or activities.

Part III of the Act specifically covers terrorist financing and creates certain specific offences as follows:

- Fund Raising – Section 12 makes it an offence to raise funds for the purpose of terrorist activities.
- Property – Section 13 makes it an offence to use and possess property for terrorist purposes.
- Funding Arrangements – Section 14 makes it an offence to enter into funding arrangements for terrorist purposes.
- Money Laundering- Section 15 makes it an offence to engage in money laundering for terrorist purposes.
- Disclosure of Information – Section 17 makes it a duty to disclose information relating to a person who is suspected of committing a terrorist financing offence. Section 19 makes it a duty to disclose information relating to the possession or control of terrorist property.

Persons who commit any of the offences in Part II of the Act are liable on conviction on indictment, to imprisonment for a term not exceeding fourteen years or to a fine or both; or on summary conviction, to imprisonment for a term ranging from six months to ten years or to a fine or both.

8. Mutual Assistance in Criminal Matters Act, 1993 (Cap 4.19)

The Mutual Assistance in Criminal Matters Act is another tool in the arsenal of the Federation to assist in narrowing the avenues that are open to the perpetrators of money laundering and terrorist financing offences. The Act was passed in 1993 and has as its main objectives, to provide assistance to Commonwealth countries and other designated territories in criminal matters.

The kind of assistance that might be provided to or by a requesting country involves a range of activities including, obtaining evidence in a matter, locating or identifying a person, assistance in tracing property and in serving documents. It should be noted that property is defined widely in the Act to include money and all other property whether real or personal, tangible or intangible in nature.

The Federation has responded to a significant number of requests to provide assistance under this Act and always seeks to provide responses to requests in a timely manner. A regulated business should be aware that its cooperation might be solicited at some point in time in order to meet the overall goals of the Act, to extend the arm of the law into another jurisdiction and vice-versa in order to be able to identify and trace the activities and assets of money launderers and terrorists and those who finance their activities.

9. Group Practice

Where a group whose headquarters is in the Federation of Saint Christopher and Nevis operates or controls branches or subsidiaries in another jurisdiction, it must:

- Ensure that such branches or subsidiaries observe these Guidance Notes or adhere to local standards if those are at least equivalent;
- Keep all such branches and subsidiaries informed as to current group policy; and
- Ensure that each such branch or subsidiary informs itself as to its own local reporting point equivalent to the FIU in the Federation of Saint Christopher and Nevis and that it is conversant with the procedure for disclosure equivalent to Appendix H.

10. What is Money Laundering?

1) The expression “money laundering” covers all procedures to conceal the origins of criminal proceeds so that they appear to have originated from a legitimate source. This gives rise to three features common to persons engaged in criminal conduct, namely they seek:

- To conceal the true ownership and origin of criminal proceeds;
- To maintain control over them; and
- To change their form.

2) There are three stages of laundering, which broadly speaking occur in sequence but often overlap:

- **Placement** is the physical disposal of criminal proceeds. In the case of many serious crimes (not only drug trafficking) the proceeds take the form of cash, which the criminal wishes to place in the financial system. Placement can be achieved by a wide variety of means according to the opportunity afforded to, and the ingenuity of, the criminal, his advisers and their network. Typically, it may include:

  a) placing cash on deposit at a bank (often intermingled with a legitimate credit to obscure the audit trail), thus converting cash into a readily recoverable debt;

  b) physically moving cash between jurisdictions;

  c) making loans in cash to businesses which seem to be legitimate or are connected with legitimate businesses, thus also converting cash into debt;

  d) purchasing high-value goods for personal use or expensive presents to reward existing or potential colleagues;

  e) purchasing the services of high-value individuals;

  f) purchasing negotiable assets in one-off transactions; or

  g) placing cash in the client account of a professional intermediary.

- **Layering** involves the separation of criminal proceeds from their source by the creation of layers of transactions designed to disguise the audit trail and provide the appearance of legitimacy. Again, this can be achieved by a wide variety of means according to the opportunity afforded to, and the ingenuity of, the criminal, his advisers and their network. Typically, it may include:

  a) rapid switches of funds between banks and/or jurisdictions;

  b) use of cash deposits as collateral security in support of legitimate transactions;

  c) switching cash through a network of legitimate businesses and “shell” companies across several jurisdictions; or

  d) resale of goods/assets.

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

Identifiable Points of Vulnerability

3) a) The criminal remains relatively safe from vigilance systems while criminal proceeds are not moving through the three stages of money laundering. Certain points of vulnerability have been identified in these stages which the launderer finds difficult to avoid and where his/her activities are therefore more susceptible to recognition, in particular:

- cross-border flows of cash;
- entry of cash into the financial system;
- transfers within and from the financial system;
- acquisition of investments and other assets;
- incorporation of companies; or
- formation of trusts.

Accordingly, a Compliance Program (Section 14 onwards) requires DNFBPs and their key staff to be most vigilant at these points along the audit trail where the criminal is most actively seeking to launder, i.e. to misrepresent the source of criminal proceeds. One of the recurring features of money laundering is the urgency with which, after a brief "cleansing", the assets are often reinvested in new criminal activity.

b) Risk Based Approach

i. To assist the overall objective to prevent money laundering and the financing of terrorism, these Guidelines adopt a risk based approach. Such an approach:

- recognizes that the money laundering and financing of terrorism threat to a relevant person varies across customers, jurisdictions, products and delivery channels;
- allows a relevant person to differentiate between customers in a way that matches risk in a particular business;
- while establishing minimum standards, allows a relevant person to apply its own approach to systems and controls, and arrangements in particular circumstances; and
- helps to produce a more cost effective system.

ii. Systems and controls will not detect and prevent all money laundering or the financing of terrorism. A risk based approach will, however, serve to balance the cost

burden placed on individual businesses and on their customers with a realistic assessment of the threat of a business being used in connection with money laundering or the terrorist financing by focusing effort where it is needed and has most impact.

11. Terrorism and the Financing of Terrorist Activity

1) Terrorists often control funds from a variety of sources around the world and employ increasingly sophisticated techniques to move these funds between jurisdictions. In doing so, they require the services of skilled professionals such as accountants, bankers and lawyers.

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

- Often only small amounts are required to commit a terrorist act. This makes terrorist funds harder to detect; and

- Terrorism can be funded from legitimately obtained income such as donations – it will often not be clear at what stage legitimate earnings become terrorist assets.

Detailed examples of methods of terrorist financing activities can be found in Appendix B

3) Public information is available to aid the verification procedures within regulated businesses. In addition to the International Standards on Combating Money Laundering and Financing of Terrorism & Proliferation (revised February 2012), DNFBPs shall take account of a document entitled “Guidance for Financial Institutions in Detecting Terrorist Financing” issued by the FATF in April 2002 and the FATF’s typologies report published annually. The document and the report are available from the FATF’s web site at www.fatf-gafi.org. The document describes methods of terrorist financing and the types of financial activities constituting potential indicators of such activity. The report contains an in-depth analysis of the methods used in the financing of terrorism. Both the document and the report will be updated regularly by FATF and regulated businesses should ensure that they take account of these updates.

4) In light of the fact that terrorist financing can originate in any country, firms are obligated to assess which countries carry the highest risks and should conduct careful scrutiny of transactions from persons or entities known to be sources of terrorist financing. (See US Embassy advisories issued by the Financial Services Regulatory Commission from time to time).

12. General Application

These Guidelines are intended to offer guidance for all DNFBPs which include:

1) Real estate agents involved in transactions for or on behalf of a client concerning the buying, leasing or selling of real estate in relation to both the purchasers and vendors of property.

2) Wholesale dealers or manufacturers in precious metals and precious stones.

3) Lawyers, notaries, other independent legal professionals and accountants, including auditing service providers who prepare or carry out transactions for their clients, including but not limited to:

    a) Buying, leasing or selling of real estate;

    b) Managing of client money, securities or other assets;

    c) Management of bank, savings or securities accounts other than as a business that meets the definition of financial institution;

    d) Organization of contributions for the creation, operation or management of companies;

    e) Creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

4) Casinos where roulette or card games are carried on in the establishment or where there is a slot machine – not including video lottery terminals – on the premises.

5) Trust and Company Service Providers, when they prepare for or carry out transactions for a client including but not limited to:

    a) Acting as a formation agent of legal persons;

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

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

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

e) Acting as (or arranging for another person to act as) a nominee shareholder for another person.

13. Compliance Requirements

A DNFBP should:

1) Establish, implement, monitor and maintain an effective Compliance Program in line with these guidelines.

2) Devise and implement relevant policies, procedures, processes and controls designed to prevent and detect potential Money Laundering and Terrorist Financing Activities. Such measures shall consider the following:

    a) Compliance Regime;

    b) Risk Assessment;

    c) Customer Due Diligence;

    d) Record retention;

    e) Training and awareness;

    f) Employee screening

    g) Detection of unusual and/or suspicious transactions;

    h) Monitoring and Reporting

3) Appoint a Compliance Officer at a Management level or a designated focal point for compliance related matters who will be responsible for the day-to-day oversight of relevant policies, procedures and controls to detect, prevent Money Laundering and Terrorist Financing.

4) Ensure that relevant policies, procedures, processes and controls are communicated to all relevant employees.

5) Establish ongoing employee training program to ensure that those employees are kept informed of new developments, including information on current anti Money Laundering, anti Terrorist Financing risks, techniques, methods and trends.

6) Ensure an independent review system that will test and assess the effectiveness of these Guidelines on a risk-sensitive basis; this review shall have a defined minimum frequency.

7) Devise and implement appropriate screening procedures to ensure that employees, customers and suppliers are not identified on any official sanctions list.

14. Compliance Program

1) A DNFBP's Senior Management shall ensure that a Compliance Program is executed and managed appropriately in accordance with these Guidelines.

2) A DNFBP shall appoint a Compliance Officer responsible for establishing and maintaining policies, procedures, processes and controls consistent with St. Kitts and Nevis' AML/CFT legislation and exercising day-to-day operational oversight of the DNFBP's compliance functions.

3) The Compliance Officer's responsibilities shall include identifying and undertaking appropriate actions on matters of Money Laundering and Terrorist Financing concerns that are identified as part of a risk assessment process or by queries of various authorities.

4) The Compliance Officer shall be responsible for:

    a) Establishing, implementing, monitoring and maintaining an appropriate ongoing program of AML/CFT prevention training and awareness and

    b) Producing annual reports to Senior Management concerning the level of compliance adherence to policies, procedures, processes and controls.

5) The Compliance Officer shall be responsible for receiving internal suspicious activity reports submitted by employees of the DNFBP, investigating the internal suspicious activity report and taking appropriate action which would include, where appropriate, making external Suspicious Activity Reports (STRs) to the Financial Intelligence Unit (FIU).

6) The Compliance Officer shall also be responsible for acting as the point of contact to the FIU and relevant agencies concerned with AML/CFT matters and responding promptly to any request for information made by the FIU or other Competent Authorities of St. Kitts and Nevis.

7) The Compliance Officer shall notify the FIU promptly regarding any communication from other authorities or regulators concerning Money Laundering or Terrorist Financing matters.

8) A DNFBP shall make appropriate provisions for any absence of the Compliance Officer and appoint a suitable Deputy to assume the responsibilities set out above.

9) The Compliance Officer shall have requisite experience and independence to act on his/her own authority, have direct access to Senior Management and have sufficient resources including appropriately trained and effective staff.

10) The Compliance Officer shall have access to relevant information concerning the DNFBP's customers, representatives of the customers, business relationships and transactions and the details of such transactions which a DNFBP contemplates or actually enters into, with or for a client or third party.

11) A DNFBP shall commission an annual report from its Compliance Officer that will report the level of compliance adherence to relevant policies, procedures, processes and controls with respect to regulatory obligations.

15. Customer Due Diligence (CDD)

1) GENERAL

A DNFBP should:

a) Properly identify its customers and maintain client identification records including reliable documentation. Such customer identification records should be made available to the FSRC or to any Competent Authority promptly upon request.

b) Adopt a risk based approach to determine the extent of additional CDD measures commensurate with the level of risk posed by the customer type, business relationship, transaction, product/service or geographical location.

c) Conduct Enhanced Due Diligence (EDD) measures when there is a suspicion of Money Laundering or Terrorist Financing or where high risk circumstances are identified.

2) TIMING

A DNFBP shall:

a) Undertake satisfactory CDD measures when:

i. Establishing a business relationship;

ii. There is any suspicion of Money Laundering or Terrorist Financing;

iii. The DNFBP has doubts about the integrity of previously obtained customer identification date;

iv. Updating the CDD information on an annual basis.

b) Verify the identity of each customer and beneficial owner when establishing a business relationship or conducting transactions for irregular customers.

3) APPLICATION

A DNFBP shall implement the following standards of CDD measures:

a) Identify and verify the identity of a customer that is a natural person, using relevant and reliable independent source documents, data or information (Identification Data);

i. The relevance and usefulness in this context of the following personal information shall be considered:

- Full name(s) used;
- Date and place of birth;
- Nationality;
- Current permanent address, including post code (any address printed on a personal account cheque tendered to open the account or render the service, if provided, should be compared with this address);
- Telephone and fax number;
- Occupation and name of employer (if self-employed, the nature of the self-employment); and
- Specimen signature of the customer (if a personal cheque is tendered to open the account or render the service, the signature on the cheque should be compared with the specimen signature).

ii. To establish identity, the following documents shall be used in descending order of acceptability:

- Current valid passport;
- National identity card;
- Armed forces identity card; and
- Driver's licence which bears a photograph.

iii. Documents which are easily obtained in any name shall not be accepted at face value without critical review. They must only be accepted where there is a satisfactory explanation as to why the documents listed in Section 15(a)(ii) are not available. Examples include:

- Birth certificates;
- An identity card issued by the employer of the applicant even if bearing a photograph;
- Credit cards;
- Business cards;
- National health or insurance cards;
- Provisional driver's licence; and
- Student union or identity cards.

iv. It is acknowledged that there will sometimes be cases, particularly involving young persons and the elderly, where appropriate documentary evidence of identity and independent verification of address are not possible. In such cases, a senior member of staff shall authorize the opening of an account only if he is satisfied with the circumstances and shall record those circumstances in the same manner and for the same period of time as other identification records.

b) If a customer is not a natural person, the DNFBP shall:

i. Identify and verify the name, address and legal status of the customer by obtaining proof of incorporation issued by the relevant authority or similar formal evidence of establishment and existence;

ii. Verify that any person purporting to act on behalf of the customer is authorized to do so and that such person's identity is properly verified;

iii. Identify the beneficial owner, taking reasonable measures to verify the identity of the beneficial owner using identification data obtained such that the DNFBP is satisfied that it recognizes who the beneficial owner(s) are;

iv. Understand the ownership and control structure of the customer; and

v. Identify the natural persons that may ultimately own and control the customer.

c) Establish and record the purpose and intended nature of the business relationship;

d) Conduct ongoing due diligence on the business relationship and apply scrutiny to transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the DNFBP's knowledge of the particular clients, their business and risk profile, including, where necessary, the source of funds;

e) Establish measures for customers who conduct large cash transactions;

f) In addition, to as stated above, in the case of casinos, specific measures to identify a customer whom the casino pays a casino disbursement.

4) A DNFBP shall ensure that identification data is kept up-to-date and may review the records of higher risk customers or business relationships as appropriate.

5) Where a DNFBP is unable to comply with any of the CDD measures, it shall not open an account, commence business relations, accept instructions or perform the transaction.

6) Where CDD obligations for existing business relationships and clients are not met, as a result of the client's refusal to comply or where the client causes unacceptable delays, the DNFBP shall terminate the business relationship and consider making a Suspicious Transaction Report STR) to the FIU.

7) CDD measures shall apply to all DNFBP's new clients. A DNFBP shall apply relevant CDD measures to existing clients in situations where:

a) The customer's documentation standards are changed substantially with the introduction of compliance requirements with these guidelines; or

b) There is a material change in the nature of the relationship with the customer; or

c) The DNFBP becomes aware that it lacks sufficient information about an existing customer or is concerned about the accuracy of information recorded.

16. Risk Assessment

A DNFBP shall:

a) Adequately assess its AML/CFT risks in relation to its customers, its business, products and services, geographical exposures and appropriately define and document its risk-based approach.

b) Maintain AML/CFT prevention policies, procedures, processes and controls that are relevant and up-to-date in line with the dynamic risk associated with its business, products and services and that of its customers.

c) Establish, implement, monitor and maintain satisfactory controls that are commensurate with the level of AML/CFT risk.

d) The FSRC shall issue relevant guidance and conduct necessary training for the proper implementation of a Compliance Program.

17. Enhanced Due Diligence (EDD)

The DNFBP shall:

a) Perform Enhanced Due Diligence (EDD) for higher risk categories of customers, business relationships or transactions.

b) Be aware of new or developing technologies that might favour and take measures to prevent their use for the purpose of Money Laundering and Terrorist Financing.

c) Apply EDD in the following circumstances:

HIGH RISK PARTIES

i. In assessing the risk in relation to Money Laundering and Terrorist Financing, A DNFBP shall give special attention to business relationships

established and transactions intended or conducted with persons and entities from or in countries that do not apply, or insufficiently apply, AML/CFT rules, as identified by:

- The Financial Services Regulatory Commission (FSRC);
- Financial Intelligence Unit (FIU);
- The Financial Action Task Force (FATF);
- Caribbean Financial Action Task Force (CFATF).

d) A DNFBP shall apply systems and controls that can appropriately identify and manage the enhanced risk associated with clients or transactions in or from countries that are prone to money laundering and terrorism.

e) A DNFBP shall make appropriate use of relevant findings issued by any of the above authorities concerning any named individuals, groups or entities that are the subject of money laundering or terrorist financing investigations or included in sanctions lists issued by international competent authorities. Regarding various individuals and entities, the DNFBP shall know prior to establishing a customer relationship:

i. The identity of the person;

ii. The type of activity/relationship he/she wants to conduct with the DNFBP;

iii. The complexity of the transaction;

iv. Whether or not the customer is representing a third party;

v. How to verify the information presented.

NON FACE-TO-FACE BUSINESS

f) When conducting non face-to-face business with clients that have not been physically present for the purposes of identification and verification, the DNFBP shall have policies, procedures, systems and controls in place to manage specific risks associated with such non face-to-face business, relationships or transactions.

g) A DNFBP shall, at a minimum, require one (1) piece of formal identification which has been certified appropriately and one formal document that will verify the physical address of the customer. Where the customer is a legal person, a DNFBP shall require documentary evidence of the continuing existence of the legal person (good standing

certificate) and a certified copy of acceptable identification and address documentation to verify the address of any person defined in 15(a).

h) A DNFBP shall ensure that adequate procedures for monitoring activity of non face-to-face business are implemented and managed effectively.

i) The FSRC shall issue relevant guidance and conduct necessary training for the implementation of CCD.

18. Outsourcing

1) A DNFBP may outsource the technical aspects of the Compliance process only to a qualified service provider, as long as such outsourcing allows for:

   i. The DNFBP to promptly obtain from the Compliance Service Provider the information under Section 13; and

   ii. The DNFBP's ability to obtain copies of Identification Data and other relevant documentation relating to CDD requirements promptly upon request.

2) The ultimate responsibility for customer identification and verification and other outsourced functions is that of the DNFBP regardless of the arrangements entered with any Compliance Service Provider.

3) A DNFBP shall ensure that there are no secrecy and data protection issues that would restrict prompt access to data or impede the full application of the Guidelines with respect to any outsourced relationship.

19. Suspicious Activity and Monitoring

1) A DNFBP should routinely monitor for and detect suspicious activity and examine its background and purpose. The following suspicious activity should be monitored:

   a) Lawyers

i. Appointing a lawyer in financial or commercial transactions and requesting the concealment of the customer's name in any of these transactions.

ii. The customer resorts to lawyers to create companies, particularly international business companies, from outside the country (offshore) in a way that shows that the objective of creating the company is to conceal the illicit source of the funds.

iii. The customer resorts to lawyers to invest in the real estate market but the purchase or sale prices are not commensurate with the real estate value.

iv. The customer requests, upon hiring a lawyer to incorporate a company, to transfer/deposit the incorporation fees or the capital to/in the bank account of the lawyer through multiple accounts that he has no relation to without a reasonable justification.

v. The lawyer manages investments portfolios, in countries allowing such conduct, and receives instructions from the customer to make buying/selling transactions that have no clear economic reason.

b) Accountants

i. The customer does not indicate concern in incurring losses or realizing extremely low profits in comparison with persons engaged in the same business. The customer remains persistent in pursuing his/her activities.

ii. High volume of foreign transfers from/to the client's accounts or the sudden increase of the revenue and cash amounts he obtains that is not consistent with his/her usual income. This type of activity occurs in a manner without any justification.

iii. Customer's receipt of cash money or high value cheques, which do not suit the volume of his/her work or the nature of his/her activity, particularly if the transactions come from persons who are not clearly or justifiably connected to the client.

iv. Unjustified amounts or deposits in the customer's account whose origin or cause is difficult to identify.

v. Disproportionate amounts, frequency and nature of transactions carried out by the customer that are not consistent with the nature of his business, profession or known and declared activity, particularly if these transactions are carried out with suspicious countries that are not connected to his/her apparent business domain.

vi. Repeated large-amount cash transactions including foreign exchange transactions or cross-border fund movement when such types of transactions are not consistent with the usual commercial activity of the customer.

c) Real Estate Agents

i. Buying or selling real estate property at a price not consistent with its actual value, whether by increase or decrease, in comparison with the market prices or the prices of similar real estate in the same area.

ii. Repeated buying of real estate properties whose prices do not suit the buyer's usual capacity according to the information available about him/her or expected from him/her (due to the nature of his/her profession or business), which creates suspicion that he/she is carrying out these transactions for other persons.

iii. Trying to register the real estate property at a price less that actual value or the amount that will be paid and pay the difference "under the table".

iv. The customer is not interested in inspecting the real estate to check its structural condition prior to the completion of the purchase operation.

v. The customer is not interested in verifying the legal status of the real estate property he/she intends to buy.

vi. Purchase of a number of real estate properties in a short period of time without expressing any interest in their location, condition, costs of repairs and otherwise.

vii. Sale of the real estate property directly after buying it at a price less that the price of purchase.

viii. The customer is not interested in putting his name on any file that may relate him/her to the property or use of different names when submitting purchase offers.

ix. Buying real estate properties in the name of another person who is not clearly or justifiably connected to the customer.

x. Replacing the buyer's name shortly before the completion of the transaction without sufficient or clear justification.

xi. To arrange the financing of purchase transactions, partially or in full, through an unusual source or an offshore bank.

d) **Dealers in precious stones and metals (jewelers and gold merchants)**

i. Customer's purchase of jewels of high value without selecting any particular specifications or with no clear justification.

ii. Customer's purchase of jewels of high value does not correspond with what is expected from him/her (upon the identification of his profession or the nature of his/her business.

iii. To regularly purchase high value commodities or large quantities of a specific commodity in a way that does not suit the usual deals carried out by the customer or the usual pattern of the business for his/her income or appearance.

iv. Attempt to recover the amount of new purchases without a satisfactory explanation or when the customer tries to sell what he/she recently bought at a price that is much less than the purchasing price.

v. Attempt to sell high value jewels at a price much less than their actual or market value.

vi. Customer's willingness to pay any price to obtain jewels of extravagant amounts without any attempt to reduce or negotiate the price.

e) Notaries

i. Customers desire to create or buy a company that has a suspicious objective, does not realize profits or does not seem to be connected to his/her usual profession or related activities, without being able to submit sufficient explanations to the notary.

ii. When a customer sells assets or real estate properties repeatedly without realizing any profit margin or submitting a reasonable explanation in this respect.

iii. The customer who creates or wishes to create different companies in a short timeframe for his own interest or the interest of other persons without reasonable financial, legal or commercial grounds.

iv. The customer's use of another person as a facade to complete a transaction without any legitimate financial, legal or commercial excuse.

f) Casinos

i. The value used is disproportionate to the customer's assumed resources in light of his/her declared profession.

ii. The outcome of the operations or the type of currencies used is disproportionate to the customer's profession.

iii. Changing the gambling routines for a certain customer in disproportion with his/her income that was declared beforehand, e.g. if he/she purchases chips for a game that he/she does not usually play or if it is observed from the objective circumstances that he/she does not seek profit or is not concerned about losing.

iv. Buying gambling chips in cash, then requesting to exchange them with a cheque from the casino.

g) General Suspicious Activity

i. The customer has an unusually comprehensive knowledge of money laundering issues and the AML Law without justification. For instance, if the customer points out he/she wishes to avoid being reported.

ii. Attempt to divide the amounts of any operations below the applicable designated threshold of reporting to the competent authorities regarding money laundering or terrorist financing suspicion.

iii. The customer has an unusual interest in the internal policies, controls, regulations and supervisory procedures and unnecessarily elaborates on justifying a transaction.

iv. When a customer has accounts with several international banks or has lately established relationships with different financial institutions in a specific country without clear grounds, particularly if this country does not apply an acceptable AML/CFT regime.

v. The customer is reserved, anxious or reluctant to have a personal meeting.

vi. The customer uses different names and addresses.

vii. The customer requests or seeks to carry out the transactions without disclosing his identity.

viii. The customer refuses to submit original documentation particularly those related to his identification.

ix. The customer intentionally conceals certain important information like his address (actual place of residence), telephone number or gives a non-existent or disconnected telephone number.

x. The customer uses a credit card issued by a foreign bank that has no branch/headquarters in the country of residence of the client while he/she does not reside or work in the country that issued said card.

xi. Cash transactions where banknotes with unusual denominations are used.

xii. Unusual transactions in comparison with the volume of the previous transactions or the activity pursued by the customer.

xiii. Unnecessarily complex transactions or those that do not seem to have an economic feasibility.

xiv. Transactions that involve a country that does not have an efficient AML/CFT regime, that is suspected to facilitate money laundering operations or where drug manufacturing or trafficking are widespread.

20. Suspicious Transaction Reporting

1) A DNFBP shall have relevant policies, procedures, processes and controls in place that would enable an employee to report to the Compliance Officer any suspicion or knowledge of Money Laundering or Terrorist Financing activity that is detected or identified.

2) If a DNFBP suspects or has reasonable grounds to suspect that funds concerning an actual or proposed transaction are the proceeds of any criminal activity or are related to Money Laundering or Terrorist Financing, the Compliance Officer shall promptly file a written Suspicious Transaction Report (STR) with the FIU (Appendix D).

3) The Compliance Officer shall ensure that every employee is aware of his/her role and duty to receive or submit internal STRs.

4) The Compliance Officer shall investigate STRs internally, build an internal report outlining the outcome of his/her investigation including the decision on whether or not to file an external STR. Where appropriate, the Compliance Officer shall submit the STR to the FIU (Appendix C).

5) Where applicable, the background and purpose of the activity in question may be examined by the Compliance Officer and the findings may be established in writing.

6) In the event the Compliance Officer concludes that no external report should be submitted to the FIU, the justification of such a decision should be documented.

7) A DNFBP shall institute disciplinary measures against any employee that fails to make an internal suspicious activity report where there is evidence for him/her to do so.

8) The FSRC may issue relevant guidance and recommend the necessary training for the implementation of Section 20.

21. Non-Disclosure of Reporting

DNFBPs, their directors, officers and employees (permanent and temporary) shall not disclose to the subject or any person other than one with a legitimate right to know or need to know, the fact that an STR or related information has been or will be reported to the Compliance Officer or the FIU.

22. Regulatory Cooperation

1) Where a DNFBP receives a request for information from any Competent Authority regarding enquiries into potential money laundering or terrorist financing activity, the DNFBP shall promptly inform the FIU in writing.

2) A DNFBP shall promptly respond to any appropriate request for information issued by the FIU.

23. Training

1) A DNFBP shall establish on-going and up-to-date relevant AML/CFT employee training that appropriately covers their obligations under the laws, regulations, policy and procedures, processes and controls.

2) A DNFBP shall establish measures to ensure that employees are kept informed and up-to-date with risk vulnerabilities, including information on current AML/CFT techniques, methods and trends.

3) A DNFBP shall ensure that training is sufficiently tailored in its content and frequency to the operations and business of the DNFBP, its employee and its clients.

4) A DNFBP shall keep employees informed on an ongoing basis of the type of suspicious activity that is pertinent to the type of business of the DNFBP and to the context of the employees' functions.

5) Except in respect of Senior Managers and the Compliance Officer whose training must be provided immediately on assumption of their duties, a DNFBP shall ensure that all relevant employees receive appropriate training within sixty (60) days of commencement of employment.

24. Record Keeping

1) A DNFBP shall maintain all records pertaining to the CDD documentation and on any transaction for at least five (5) years following the establishment of the relationship or the completion of the transaction, regardless of whether the account or business relationship is ongoing or has been terminated.

2) Where maintenance of customer records is outsourced to qualified service providers in accordance with Section 15, DNFBPs shall take reasonable steps to ensure that such records are held in a manner that conforms to these Guidelines.

3) A DNFBP shall maintain information, correspondence and documentation for customer identification and verification and associated due diligence for a period of at least five (5) years from the end of the business relationship with the client or the last transaction conducted.

4) A DNFBP shall maintain records in accordance with Section 20 concerning the internal reporting of unusual or suspicious transactions and all records of investigations of those reports, together with the decision made, should be retained for at least a period of five (5) years after the report has been made.

5) A DNFBP shall maintain records including dates of training sessions, a description of training provided and names of employees that received training for a period of at least five (5) years from the date on which training was received.

6) A DNFBP shall maintain records of annual reports and any other reports that highlight the level of compliance, deficiencies and actions, including reports submitted to Senior Management.

7) The transactions records and other identification data shall be made available to the FSRC, FIU or any other Competent Authority upon request.

Appendix A - Examples of laundering schemes uncovered

Account opening with drafts

An investigation into part of an international money laundering operation involving the UK revealed a method of laundering using 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 an exchange bureau (cambio houses). Drafts, frequently referred to as cambio drafts or cambio cheques, were purchased in sums ranging from $ 5,000.00 to $ 500,000.00 drawn on Mexican or American banks. The drafts were then used to open accounts in banks in the UK with funds later being transferred to other jurisdictions as desired.

Bank deposits and international transfers

An investigation resulting from a disclosure identified an individual who was 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 and a large sum was 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 USA. Over an 18-month period a total of £ 2,000,000.00 was laundered and invested in property.

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

Bogus Property Company

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

Theft of company funds

A fraud investigation into the collapse of a wholesale supply company revealed that the director had stolen very substantial sums of company funds, laundering the money by issuing company cheques to third parties. These cheques 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 and 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.

Deposits and sham loans

Cash collected in the USA 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 case by air to London, where it was paid into a branch of a financial institution in Jersey. Enquiries in London by HM Customs and Excise revealed that internal bank transfers had been made from the UK to Jersey where 14 accounts had been opened in company names using local nominee directors. The funds were repatriated to North America with the origin disguised, on occasions in the form of sham loans to property companies owned by the principals, either using the Jersey deposits as collateral or transferring it back to North America.

Cocaine lab case

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

Local research identified the customer as being previously suspected of local cocaine dealing. Production orders were obtained and it was found that his business could not have generated the substantial wealth that the customer displayed; in addition his business account was being used to purchase chemicals known to be used in refining cocaine. Further enquiries connected the man to storage premises which, when searched by police, were found to contain a cocaine refining laboratory, the first such discovery in Europe.

Currency exchange

Information was received from a financial institution about a non-account holder who had visited on several occasions, exchanging cash for foreign currency. He was known to have an account at another branch nearby and this activity was neither explained nor consistent with his account at the other branch. The subject of the disclosure was found to have previous convictions for drugs offences and an investigation ensued. The subject was arrested for importing cannabis and later convicted.

Cash deposits

Information was submitted about a customer who held two accounts at branches of the same financial institution in the same area. Although he was unemployed it was noted that he had deposited £ 500-600 cash every other day It was established that he held a third account and had placed several thousand pounds on deposit in Jersey. As a result of these investigations, he was arrested and later convicted for offences related to the supply of drugs.

Bank complicity

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

Information received led to a manager of the financial institution being suspected of being in complicity with the trafficker and his associates. He was arrested and later convicted of an offence of unlawful disclosure (tipping-off) and sentenced to 4 years' imprisonment.

Single premium life policy with offshore element

Enquiries by the police established that cash derived from drug trafficking was deposited in several UK bank accounts and then transferred to an offshore account. The trafficker entered into a £50,000.00 life insurance contract, having been introduced by a broking firm. Payment was made by two separate transfers from the offshore account. It was purported that the funds used for payment were the proceeds of overseas investments. At the time of the trafficker's arrest, the insurer had received instructions for the early surrender of the contract.

Corporate instrument

Cash from street sales of heroin and amphetamines was used to shore up an ailing insurance brokerage company. A second company was bought and used to purchase real estate for improvement and resale. Ownership of the real estate was transferred from the company to the principal conspirator. The process was halted by the arrest of the offenders who were convicted of drug and money laundering offences.

Cash purchases or investments

A disclosure was made by a UK financial institution concerning two cash payments of £ 30,000.00 and £ 100,000.00 for the purchase by a customer of investment bonds. Both investments were undertaken by a salesman of the financial institution following home visits to the customer on separate dates. The cash paid for the bonds was mainly in used notes. Enquiries by the police established that the prospective investor and his wife were employed by a note-issuing bank to check used bank notes before destruction or recirculation. A further investigation of the suspects and their families identified lifestyles way beyond their respective salary levels. The outcome was a successful prosecution under the Theft Act and a prison sentence for the principal offender.

The Spence money- laundering network in New York

A fascinating example of money laundering was uncovered in New York in 1994. It involved a network of 24 people, including the honorary consul-general for Bulgaria, a New York city police officer, two lawyers, a stockbroker, two rabbis, a fire-fighter and two bankers in Zurich. A law firm provided the overall guidance for the laundering effort while both a trucking business and a beer distributorship were used as cover. The Bulgarian diplomat, the fire-fighter and a rabbi acted as couriers, picking up drug trafficking

proceeds in hotel rooms and parking lots, while money was also transported by Federal Express to a New York trucking business. The two lawyers subsequently placed the money into bank accounts with the assistance of a Citibank assistant manager. The money was then wired to banks in Europe, including a private bank in Switzerland, at which two employees remitted it to specific accounts designated by drug traffickers. During 1993 and 1994 a sum of between $ 70 million and $ 100 million was laundered by the group. It turned out, however, that the bank had supplied a suspicious activity report to law enforcement agencies. Furthermore, the assistant bank manager, although initially arrested, was subsequently reinstated and still works for Citibank. In the final analysis, this seems to have been a case where a suspicious activity report played a critical role in the downfall of the money- laundering network.

The Sagaz case

In March 1998, Gabriel Sagaz, the former president of Domecq Importers, Inc., pleaded guilty to a charge of conspiracy to defraud for actions that had taken place between 1989 and August 1996. Sagaz and several colleagues had embezzled over $13 million directly from the company and received another $ 2 million in kick-backs from outside vendors who invoiced for false goods and services. Sagaz approved the ph ney invoices and, after the vendors were paid by Domecq Importers, they issued cheques to shell corporations controlled by Sagaz and his colleagues. The cheques were deposited in offshore bank accounts opened by Sagaz and his colleagues, thereby adding tax evasion to the charges.

The Harrison (Iorizzo) oil gasoline tax fraud case

In June 1996, the United States Department of Justice announced that Lawrence M. Harrison, formerly known as Lawrence S. Iorizzo, had been sentenced to over 15 years in prison for a tax fraud in Dallas. He had been convicted in March 1996 on charges of motor fuel excise tax evasion, conspiracy, wire fraud and money laundering. Iorizzo had been the key figure in motor fuel tax evasion schemes that had proved so lucrative for Russian criminal organisations in New York, New Jersey and Florida in the 1980s and that also included payments to some of the New York mafia families. After going into witness protection, Harrison along with other family members and associates had purchased a small Louisiana corporation, Hebco Petroleum, Inc, in 1988 and became involved in the Dallas/Fort Worth wholesale diesel fuel and gasoline markets.

Although Hebco's invoices included state and federal taxes, the company kept this revenue. According to the indictment, between June 1989 and January 1990, Hebco grossed approximately $26 million in fuel sales. During the same period, the company sent approximately $3 million from Texas bank accounts to a Cayman Islands account from which it was forwarded to European bank accounts, apparently to fund a similar fraud scheme in Belgium.

BAJ Marketing

In March 1998, the United States Attorney's office in New Jersey asked for a temporary restraining order to stop four offshore corporations in Barbados from marketing fraudulent direct mail schemes to consumers in the United States. The order was directed against BAJ Marketing Inc., Facton Services Limited, BLC Services Inc. and Triple Eight International Services. With no offices or sales staff in New Jersey or

anywhere else in the United States, the businesses tricked consumers into sending "fees" to win prizes of up to $10,000.00 - prizes that never materialized. The companies were owned or controlled by four individuals from Vancouver, British Columbia, all of whom had been indicted in Seattle for operating an illegal gambling scheme.

The defrauding of the National Heritage Life Insurance Corporation

In 1997, a case in Florida involving fraud and money laundering was brought to trial. Over a 5-year period, five people had used various schemes to defraud the National Heritage Life Insurance Corporation. One of the counts was against a former attorney who had transferred around $ 2.2 million to an offshore account in the Channel Islands.

A lawyer's case

In one case in the United States, used by the Financial Action Task Force to illustrate the role of professionals such as attorneys in money laundering, a lawyer created a sophisticated money laundering scheme that utilized 16 different domestic and international financial institutions, including many in offshore jurisdictions. Some of his clients were engaged in white-collar crime activities and one had committed an $80 million insurance fraud. The laundering was hidden by "annuity" packages, with the source of funds being "withdrawals" from these. The lawyer commingled client funds in one account in the Caribbean and then moved them by wire transfer to other jurisdictions. Funds were transferred back to the United States either to the lawyer's account or directly to the client's account. The lawyer also arranged for his clients to obtain credit cards in false names, with the Caribbean bank debiting the lawyer's account to cover the charges incurred through the use of these cards.

Additionally, attention is drawn to the 100 cases from the Egmont Group. This is a compilation of 100 sanitized cases on successes and learning moments in the fight against money laundering produced by the Financial Intelligence Unit members of the Egmont Group. This report is available at www.ncis.co.uk.

Cases relating to terrorist financing can be found in Appendix B of these notes.

APPENDIX B – Examples of Terrorist Financing

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

EXAMPLES OF METHODS OF TERRORIST FINANCING

i. Donations

It is common practice in certain communities for persons to make generous donations to charity. a “zakat”, one tenth of one’s income, to charity. There should be no assumption that such donations bear a relation to terrorist funding. However, donations continue to be a lucrative source of funds for terrorist financing. Such donations are often made on an irregular basis.

ii. Extortion

This form of raising money continues to be one of the most prolific and highly profitable. Monies are usually raised from within the community of which the terrorists are an integral part and are often paid as protection money. Eventually, extortion becomes a built in cost of running a business within the community.

iii. Alternative Remittance

Alternative Remittance consists of money or value transmission services and include informal systems or networks that fail to obtain a license/register. Informal money or value transfer systems have shown themselves vulnerable to misuse for money laundering or terrorist financing purposes. A financial service is provided whereby funds or value are moved from one geographic location to another. However, in some jurisdictions, these informal systems have traditionally operated outside the regulated financial sector in contrast to the “formal” money remittance/transfer services. Some examples of informal systems include the parallel banking system found in the Americas (often referred to as the “Black Market Peso Exchange”), the hawala or hundi system of South Asia, and the Chinese or East Asian systems.

iv. Smuggling

Smuggling across a border has become one of the most profitable ventures open to terrorist organisations. Smuggling requires a co-ordinated, organised structure, with a distribution network to sell the smuggled goods. Once set up, the structure offers high returns for low risks. Criminal partners benefit from their involvement and considerable amounts are often made available for the terrorist organisation.

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

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

v. Charities

There are known cases of charities being used to raise funds for terrorist purposes. They have not always published full accounts of the projects which their fund raising has helped to finance. In some cases, charities have strayed outside the legal remit for which they were originally formed.

vi. Drugs

The provision of drugs can be a highly profitable source of funds and is used by some groups to finance other activities. Many terrorist groups are not directly

involved in the importation or distribution but, in order for the drug suppliers to operate within a certain area or community, a levy would have to be paid. Such extortion, often known as protection money, is far less risky than being responsible for organising the supply and distribution of drugs.

USE OF THE FINANCIAL SYSTEM

Terrorists and those financing terrorism have used the following services and products to transfer and launder their funds:

i. bank accounts (including the targeting of previously dormant accounts which are re-activated);
ii. electronic transfers (wire transfers); and
iii. money services businesses.

The case studies below provide examples of the trends outlined above.

EGMONT COLLECTION OF SANITISED CASES RELATED TO TERRORIST FINANCING

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

Case 1: “Donations” support terrorist organisation

A terrorist organisation collects money in Country A to finance its activities in another country. The collecting period is between November and January each year. The organization collects the funds by visiting businesses within its own community. It is widely known that during this period the business owners are required to “donate” funds to the cause. The use or threat of violence is a means of reinforcing their demands. The majority of businesses donating funds have a large cash volume. All the money is handed over to the collectors in cash. There is no record kept by either the giver or the receiver. Intimidation prevents anyone in the community from assisting the police, and the lack of documentation precludes any form of audit trail. It is estimated that the organisation collects between USD 650,000.00 and USD 870,000.00 per year. The money is moved out of the country by the use of human couriers.

Case 2: Contribution payments support terrorist organisation

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

Case 3: Smuggling supports terrorist organization

A terrorist organisation is involved in smuggling cigarettes, alcohol and petrol for the benefit of the organisation and the individuals associated with it. The goods are purchased legally in Europe, Africa or the Far East and then transported to Country B. The cost of the contraband is significantly lower than it is in Country B due to the

different tax and excise duties. This difference in tax duties provides the profit margin. The terrorist organization uses trusted persons and limits the number of persons involved in the operation. There is also evidence to point to substantial co-operation between the terrorist organisation and traditional organised crime.

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

The smuggler also sometimes gives the funds to legitimate businesses that are not associated with the smuggling operation. The funds enter the banking system as part of a company's normal receipts. Monies are passed through various financial institutions and jurisdictions.

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

An individual purchases an expensive new car. The individual obtains a loan to pay for the vehicle. At the time of purchase, the buyer also enters into a medical insurance policy that will cover the loan payments if he were to suffer a medical disability that would prevent repayment. A month or two later, the individual is purportedly involved in an "accident" with the vehicle, and an injury (as included in the insurance policy) is reported. A doctor, working in collusion with the individual, confirms injury. The insurance company then honours the claim on the policy by paying off the loan on the vehicle. Thereafter, the organisation running the operation sells the motor vehicle and pockets the profit from its sale. In one instance, an insurance company suffered losses in excess of USD 2 million from similar fraud schemes carried out by terrorist groups.

Case 5: Credit card fraud supports terrorist network

One operation discovered that a single individual fraudulently obtained at least twenty-one Visa and MasterCard using two different versions of his name. Seven of those cards came from the same banking group. Debts attributed to those cards totaled just over USD 85,000.00. Also involved in this scheme were other manipulations of credit cards, including the skimming of funds from innocent cardholders. This method entails copying the details from the magnetic strip of legitimate cards onto duplicate cards, which are used to make purchases or cash withdrawals until the real cardholder discovers the fraud. The production of fraudulent credit cards has been assisted by the availability of programmes through the Internet.

Case 6: High account turnover indicates fraud allegedly used to finance terrorist organizations

An investigation in Country B arose as a consequence of a suspicious transaction report. A financial institution reported that an individual who allegedly earned a salary of just over USD 17,000.00 per annum had a turnover in his account of nearly USD 356,000.00. Investigators subsequently learned that this individual did not exist and that the account had been fraudulently obtained. Further investigation revealed that the account was linked to a foreign charity and was used to facilitate the collection of funds for a terrorist organization through a fraud scheme. In Country B, the government

provides funds to charities in an amount equivalent to 42 percent of donations received. Donations to this charity were being paid into the account under investigation, and the government grant was being claimed by the charity. The original donations were then returned to the donors so that effectively no donation had been given to the charity. However, the charity retained the government funds. This activity resulted in over USD 1.14 million being fraudulently obtained.

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

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

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

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

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

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

The FIU analyzed the financial movements relating to the individual's accounts using records requested from the bank. It appeared that both of the accounts had been opened by the individual in 1990 and had been fed mostly by cash deposits. In March 2000 the individual made a sizable transfer from his savings account to his cheque

account. These funds were used to pay for a single premium life insurance policy and to purchase certificates of deposits.

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

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

Finally, the anti-money laundering unit in the individual's country of origin communicated information related to suspicious operations carried out by him and by the companies that received the transfers. Many of these names also appeared in the files of the FIU.

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

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

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

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

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

According to information obtained by the FIU, one of the accounts held by the company appeared to have received large US dollar deposits originating from companies active in the diamond industry. One of the directors of the company, a citizen of Country C but

residing in Africa, maintained an account at another bank in Country C. Several transfers from foreign countries were mainly in US dollars. They were converted into the local currency and transferred to foreign countries and to accounts in Country C belonging to one of the two individuals who were the subject of the suspicious transaction reports.

Police information obtained by the FIU revealed that an investigation had already been initiated relating to these individuals and the trafficking of diamonds originating from Africa. The large funds transfers by the diamond trading company were mainly sent to the same person residing in another region. Police sources revealed that this person and the individual that had cashed the cheques were suspected of buying diamonds from the rebel army of an African country and then smuggling them into Country C on behalf of a terrorist organisation. Further research by the FIU also revealed links between the subjects of the suspicious transaction report and the individuals and companies already tied to the laundering of funds for organised crime.

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

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

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

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

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

Suspicious transaction reports identified an import/export business, acting as an unlicensed money transmitter/remittance company, generating USD 1.8 million in outgoing wire transfer activity during a five-month period. Wire transfers were sent to beneficiaries (individuals and businesses) in North America, Asia and the Middle East. Cash, cheques and money orders were also deposited into the suspect account totalling approximately USD 1 million. Approximately 60 percent of the wire transfers were sent to individuals and businesses in foreign countries, which were then responsible for disseminating the funds to the ultimate beneficiaries. A significant portion of the funds was ultimately disseminated to nationals of an Asian country residing in various countries. Individuals conducting these transactions described the business as involved

in refugee relief or money transfer. The individual with sole signatory authority on the suspect account had made significant deposits (totaling USD 17.4 million) and withdrawals (totaling USD 56,900.00) over an extended period of time through what appeared to be 15 personal accounts at 5 different banks.

Case 13: Use of cash deposits below the reporting threshold

.

A pattern of cash deposits below the reporting threshold caused a bank to file a suspicious transaction report. Deposits were made to the account of a bureau de change on a daily basis totaling over USD 341,000.00 during a two and a half month period. During the same period, the business sent 10 wire transfers totaling USD 2.7 million to a bank in another country. When questioned, the business owner reportedly indicated he was in the business of buying and selling foreign currencies in various foreign locations, and his business never generated in excess of USD 10,000.00 per day. Records for a three-year period reflected cash deposits totaling over USD 137,000.00 and withdrawals totaling nearly USD 30,000.00. The business owner and other individuals conducting transactions through the accounts were nationals of countries associated with terrorist activity. Another bank made a suspicious transaction report on the same individual, indicating a USD 80,000.00 cash deposit, which was deemed unusual for his profession. He also cashed two negotiable instruments at the same financial institution for USD 68,000.00 and USD 16,387.00.

Appendix C – Possible Money Laundering/Terrorist Financing Suspicion - Internal report form (Part 1)

INTERNAL REPORT FORM (PART 1)

Name of Reporting Officer: _____

Name of customer: _____

Full account name (s): _____
Account no (s): _____

Date (s) of opening: _____

Date of customer's birth: _____ Nationality: _____

Passport number: _____

Identification and references: _____

Customer's address: _____

_____

Details of transactions arousing suspicion: _____

As relevant: _____ Amount (currency) _____ Date of receipt ___ Source(s) of funds ___
_____
_____
_____

Other relevant information: _____
_____
_____

Compliance Officer*: _____
_____

Senior management approval: _____
* *The Compliance Officer should briefly set out the reason for regarding the transactions to be reported as suspicious or, if he decides against reporting, his reasons for that decision.*

Notes:
Continuing vigilance in the prevention of money laundering and terrorist financing is a duty established by the Saint Christopher and Nevis Money Laundering and Anti-Terrorism Laws, Regulations and Guidance Notes. Where staff have suspicions about the possibility of money laundering or terrorist financing ,this form should be completed and handed to their manager, who will conduct preliminary enquiries and pass the report to the Compliance Officer. You should ensure that you get a written confirmation of receipt of your report from the Compliance Officer as evidence that you have met your obligations under the law.

Tipping Off: Remember that it is a ***criminal offence*** to disclose ***any*** information to ***any*** other person that is likely to prejudice an investigation and this might include disclosure of the existence of an internal report. You should always keep client affairs confidential and particularly the existence of money laundering suspicions. ***Money laundering or terrorist financing suspicions should not be discussed with clients***.

Appendix C – Possible Money Laundering/Terrorist Financing Suspicion - Internal report form (Part 2)

INTERNAL REPORT FORM (PART 2) REF #:

The Compliance Officer will return a copy of the bottom section of this form to the member of staff making the initial report and to the manager who has conducted the preliminary enquiries.

Action:

○ No further action required ○ Further enquiries required

○ Recommend that a Suspicious Transaction Report be made to the FIU

Reasons for action to be taken attached.

- Suspicious Transaction Report made dated:
- No Suspicious Transaction Report made, report process closed date:

Signed: _____ Dated: _____

POSSIBLE MONEY LAUNDERING/TERRORIST FINANCING SUSPICION

REF #:

Report made by: _____ Date: _____

Name of customer: _____

Full account name (s): _____

Account no (s): _____

Manager:_____

Report dated:_____

I acknowledge receipt of your internal report as detailed above.

Signed: _____Dated: _____

Appendix D - Disclosure to the FIU

DISCLOSURE TO FIU

· It would be of great assistance to the **FIU** if disclosures were made in the standard form at the end of this Appendix.

· Disclosures should be delivered in sealed and confidential envelopes by hand, by post, or, in urgent cases, by fax.

· The quantity and quality of data delivered to the **FIU** should be such as:

- to indicate the grounds for suspicion;
- to indicate any suspected offence; and
- to enable the **FIU** to apply for a court order, as necessary.
- The receipt of disclosure will be acknowledged by the **FIU.**
- Such disclosure will usually be delivered and access to the disclosure be made available only to an appropriate investigating or other law enforcement agency. In the event of prosecution the source of data will be protected as far as the law allows.
- The **FIU** should give written orders to the reporting institution to refrain from completing the transaction for a period not exceeding seventy-two hours. In conducting its investigation the **FIU** will not approach the customer. *When the FIU forwards a disclosure to the appropriate investigating authority, the authority will make discreet enquiries and not approach the customer unless criminal conduct is identified.*
- The **FIU** should seek additional data from the reporting institution and other sources with or without a court order. Enquiries should be made discreetly to confirm the basis of a suspicion.
- The **FIU** will, so far as possible and on request, promptly supply information to the reporting institution to enable it to be kept informed as to the current status of its disclosure or a particular investigation resulting from its disclosure.
- It is an important part of the reporting institution's vigilance policy / systems that all contacts between its departments and branches and the **FIU** be copied to the Compliance Officer so that he can maintain an informed overview.

SUSPICIOUS TRANSACTION REPORT

(In accordance with the Proceeds of Crime Act Cap. 4.28 and the Anti-Terrorism Act, Cap. 4.02)

Name and address of institution: _____
_____

Sort code: _____
_____

STRICTLY PRIVATE AND CONFIDENTIAL

Your ref: _____ Our ref: _____ Date: _____

The St. Kitts & Nevis Financial Intelligence Unit,
Second Floor
Ministry of Finance
Church Street
P. O. Box 1822,
Basseterre,
St. Kitts,
East Caribbean.
Telephone: 1 869 466 3451 Facsimile: 1 869 466 4945
E mail: sknfiu@thecable.net

Category: (*for official use only)* _____

Subject's full name (s) _____

Address _____

Telephone _____ Telephone _____
(home) (work)
Occupation _____ Employer _____

Date (s) of birth _____

Account / product number

Date account / product opened

Other relevant information (*please include details of identification and / or references taken, associated parties, addresses, telephone numbers, etc.)*

_____
_____
_____
_____

Reasons for suspicion _____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
_____
_____
_____

Contact name _____ Telephone _____

Signed _____

When submitting this report, please append any additional material that you may consider suitable and which may be of assistance to the recipient, i.e. bank statements, vouchers, international transfers, inter-account transfers, telegraphic transfers, details of associated accounts and products etc.

Notes:
1. Please complete a separate form in respect of each verification subject.
2. If you have any questions regarding the completion of this form please contact the