Anti-Money Laundering – Counter Financing of Terrorism (AML/CFT)

Guidance Notes

ANTI-MONEY LAUNDERING GUIDELINES

(REVISED EDITION)

Pursuant to Section 9 of the Money Laundering (Prevention) Act 8 of 2011

To Give Practical Guidance to
Financial Institutions and other Scheduled Entities
in Dominica in the Prevention, Detection and Reporting
of Money Laundering Activities

2013

Money Laundering Supervisory Authority
c/o Financial Services Unit
Ministry of Finance
5th Floor, Financial Centre
Roseau
Commonwealth of Dominica
Tel. No. 1 (767) 266 3578/3514/3558
E-mail: fsu@dominica.gov.dm

Table of Contents

ANTI-MONEY LAUNDERING GUIDANCE NOTES
PART I

FOREWORD

1. These Anti-Money Laundering Guidelines have been issued by the Money Laundering Supervisory Authority after consultation with the private sector. It provides for standards, policies and procedures which should be adopted by financial institutions and those involved in activities listed in Part II in the schedule to the Money Laundering (Prevention) Act No. 8 of 2011 in order to maintain the integrity of Dominica's financial sector in respect of money laundering. It also reflects best practice internationally and implements recommendations of the Financial Action Task Force, the Caribbean Financial Action Task Force and where applicable, Dominica's anti-money laundering legislation. The Guidelines will be considered by the courts in determining whether a financial institution and / or a person has complied with the money laundering regulations.

2. The Guidelines incorporate the views expressed and recommendations made by the private sector to ensure that Dominica maintains the highest international standards to counter money laundering. In formulating this Guide, the valuable participation of the following organisations was obtained: onshore banks, offshore banks, credit union movement, and authorised agents of offshore banks.

3. Professional associations and financial institutions may adopt more stringent guidelines than those provided in these Guidelines. Moreover, further detailed practical guidelines may be provided to members of these associations where necessary.

4. The Guidelines are subject to continuing review and may be amended as circumstances require.

SECTION I: THE INTERNATIONAL BACKGROUND

INTRODUCTION

5. On December 12, 1997 Dominica became a member of the Caribbean Financial Action Task Force ("CFATF") by signing the Memorandum of Understanding of this organisation. The CFATF was the first regional grouping, which adopted the anti-money laundering recommendations of the Financial Action Task Force ("FATF"). As a member of the CFATF, Dominica is subject to periodic evaluations of its anti-money laundering mechanisms and efforts. These Guidelines are part of the continuing commitment to meet the objectives of the CFATF and the FATF in keeping with the laws of Dominica.

FINANCIAL ACTION TASK FORCE ("FATF")

6. The FATF was established in 1989 as an inter-governmental organisation under the aegis of the Group of Seven Industrialised Countries and the President of the Commission of the European Community to develop an international approach to combating drug related money laundering. Its strategy was to encourage international adoption and implementation of legislation in compliance with the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances and to enhance multilateral legal assistance. Its membership is now closed at 32 members and 2 international organisations (see Appendix 4).

7. The FATF 40 Recommendations set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. Countries have diverse legal, administrative and operational frameworks and different financial systems, and so cannot all take identical measures to counter these threats. The FATF Recommendations, therefore, set an international standard, which countries should implement through measures adapted to their particular circumstances. The FATF Standards comprise the Recommendations themselves and their Interpretive Notes, together with the applicable definitions in the Glossary.

8. The FATF implements a programme of mutual evaluation of its members and assessment of compliance with its objectives by non-member countries.

CARIBBEAN FINANCIAL ACTION TASK FORCE ("CFATF")

9. In June 1990, 15 Caribbean states plus five members of the Financial Action Task Force with affiliations in the region met in conference in Aruba and produced 21 recommendations, 19 of which were eventually adopted as CFATF recommendations. In June 1992 a second regional meeting addressed the areas of legal, financial, political and technical assistance in combating money laundering. It provided detailed recommendations, which were presented at a ministerial meeting convened in Kingston, Jamaica in November 1992. 20 Caribbean states plus the FATF affiliates participated. An accord was agreed embodied in the

Kingston Declaration on money laundering endorsing the implementation of the 1988 United Nations Vienna Convention, the Organisation of American States Model Regulations, the 40 FATF Recommendations and the 19 Regional Specific Objectives.

10. In October 1996, 21 countries signed a Memorandum of Understanding and a Mission Statement formulating its mission, organisation and membership requirements. The countries which have signed the Memorandum of Understanding and are presently members of CFATF and the 6 Co-operating and Supporting Nations are listed in Appendix 5.

11. The CFATF also has a rolling programme of mutual evaluations. Dominica was last subject to an evaluation by its CFATF peers in September 2003.

THE BASLE STATEMENT OF PRINCIPLES

12. In December 1988, the Basle Committee of the Bank for International Settlements issued a Statement of Principles for the prevention of criminal use of financial systems. One of the cornerstones of this Statement is the ***know your customer*** principle (15) which is progressively being implemented by the banking community worldwide, including Dominica. The Statement of Principles sets out to reinforce existing best practices among banks particularly with regard to customer identification, record keeping, staff training, control systems, compliance with laws and regulations, and cooperation with law enforcement authorities. The Basle Customer Due Diligence Paper was published in October 2001 setting out detailed customer due diligence guidelines. The paper was ratified at the International Concordat on Banking Supervision in Capetown in September 2002. The ECCB was party to this ratification. The paper is also relevant to non-bank financial institutions and also introduced the concept of the Politically Exposed Person (PEP).

SECTION II: INTRODUCTION

THE PURPOSE OF THE GUIDELINES

13. The importance of the international financial services business industry in the economic diversification strategy for Dominica requires vigilance that its financial institutions and professional service providers are not misused, particularly as the provision of services such as banking, credit unions, insurance, trust, company formation and management, securities, mutual funds and real estate may be perceived as attractive targets for money launderers. Compliance with these Guidelines will assist those involved in financial transactions in identifying attempts to launder criminal proceeds, and avoiding legal, reputation and financial risk. The money laundering process will often present opportunities for recognition of its true nature if financial service providers and financial institutions are alert to the dangers of involvement and have procedures and controls in place to prevent and detect it. The ***placement*** of cash and other monetary instruments into the financial system and transfers within it are stages at which the money launderer is the most vulnerable to discovery.

14. One of the best methods of preventing and deterring money laundering is a **sound knowledge of a customer's business and expected volume and pattern of financial transactions and commitments.** Thus adoption of procedures by which relevant service providers, including financial institutions, ***"know their customer"*** is not only a principle of good business but also an essential tool to avoid involvement in money laundering.

15. This Guidelines represents good industry practice relating to financial transactions. The Government and the MLSA will, however, expect licensees to observe the Guidelines as a matter of prudent business practice in accordance with section 9 of the Money Laundering (Prevention) Act No. 8 of 2011. Failure to observe its provisions may be seen as exposing licensees to reputation, legal and financial risk and thus contrary to the safety and soundness of institutions leading to possible sanction by the FSU. Financial institutions are therefore urged to implement all of its guidelines in respect of controls, procedures, particularly those relating to the identification of clients, source of funds and staff training. This is a necessary first step to ensure compliance with the highest international standards.

THE FORMAT OF THE GUIDELINES

16. The Guide is structured to provide: general background on the subject of money laundering; introductory background and the scope of the guide: sections I - III; an outline of the principal money laundering offences in Dominica's legislation - Section IV; the principles governing policies for internal controls and procedures for verification of client identity and verification of customer identity - Sections V and VI; policies for

staff training and education programmes - Section VII; policies for record keeping - Section VIII; and procedures for recognising and reporting suspicious transactions - Section IX.

17. The specific sections in Dominica's legislation dealing with the principal money laundering offences are set out in Appendix 1.

18. Appendix 2 provides a standard form, which may be used in any report to the Financial Intelligence Unit of a suspicious transaction.

Appendices 6 to 10 provide examples of suspicious activities relating to financial service providers and non-financial businesses and professions. Appendix 11 provides guidance on Accounts Under Investigation or Legal Proceedings, Appendix 12 provide information sources which may be used and Appendix 13 includes guidance for certification of identification documents.

DEFINING MONEY LAUNDERING

19. The Money Laundering Prevention Act No. 8 of 2011 and the Proceeds of Crime Act No. 4 of 1993 address specific offences relating to dealings with the proceeds of crime. These offences (set out in Appendix 1) are summarized in Section (IV). (Act No. 8 of 2011 has been amended by Act No. 5 of 2013).

20. Money laundering is essentially the process by which the direct or indirect benefit of crime is channelled through financial transactions and institutions to conceal its true origin and ownership. Criminals are thereby enabled to mask the derivation of assets so that they appear to have originated from legitimate sources.

21. Increasingly complex and sophisticated methods of money laundering are now employed often utilizing structures with legitimate businesses, as well as "shell" or sham corporations.

22. Money laundering may involve three stages, which sometimes overlap. Each stage may involve a complex pattern of transactions:

22.1 **Placement**: the conversion of cash proceeds from crime. In a number of serious crimes, the criminal may be faced with the dilemma of disposing of cash proceeds (often in small denominations such as when drug trafficking is involved). Typically, this may be done by deposit in the banking system or exchange for value items.

22.2 **Layering:** separating the proceeds of crime from their source by creating sometimes complex layers of financial transactions designed to mask their origin, obscure the audit trail and thus hamper the investigation, reconstruction and tracing of proceeds; for example by international wire transfers using nominees or "shell" and bearer share companies, moving in and out of investment schemes or repaying credit from the direct or indirect proceeds of crime.

22.3 **Integration**: placing the laundered proceeds back into the economy as apparently legitimate business funds; for example by realising property or legitimate business assets, redeeming shares or units in collective investment schemes acquired with criminal proceeds, switching between forms of investment or surrendering paid up insurance policies.

23. Retail schemes directed to the public in which cash is used to purchase investments make the public particularly vulnerable. Financial institutions dealing directly with the public provide a target for the initial disposal of cash proceeds derived from crime and the impeding of tracing the source of funds. Offshore businesses accepting cash are particularly at risk of being involved in money laundering. **Investment and foreign deposits in the offshore banking system should not be predominantly cash-based.** The risk is therefore more likely that service providers and financial institutions may be used at the layering and integration stages of money laundering.

SECTION III: THE SCOPE OF THE GUIDELINES

WHO AND WHAT SERVICES ARE GOVERNED BY THE GUIDELINES

Financial Services Providers and Relevant Financial Transactions

24. The Guidelines applies to "Financial Services Providers" who for these purposes provide the following services (Money Laundering (Prevention) Act, 8 of 2011, Part I and Part II of the Schedule):

24.1 "Banking business" and "financial business" as defined in the Banking Act, 16 of 2005;

24.2 "Banking business" as defined in the Offshore Banking Act, 8 of 1996;

24.3 Venture risk Capital;

24.4 Money transmission services;

24.5 Issuing and administering means of payments (e.g. credit cards, travellers' cheques and bankers' draft);

24.6 Guarantees and commitments;

24.7 Trading for own account or for account of customers in-

(a) money market instruments (e.g. cheques, bills, certificates of deposits, commercial paper, etc.);

(b) foreign exchange;
(c) financial and commodity-based derivative instrument (e.g. options, interest rate and foreign exchange instruments etc.);
(d) transferable or negotiable instruments;

24.8 Money broking;

24.9 Money lending and pawning;

24.10 Money exchange (e.g. *casa de cambio*);

24.11 Mutual Funds;

24.12 Credit unions;

24.13 Building societies;

24.14 Trust business;

24.15 Insurance business;

24.16 Real estate business;

24.17 Car dealership;

24.18 Casinos (gaming houses)

24.19 Courier services;

24.20 Jewellery business;

24.21 Internet gaming & wagering services;

24.22 Management companies;

24.23 Asset management and advice custodial services;

24.24 Nominee service;

24.25 Registered Agents;

24.26 Any business transaction conducted at a post office involving money orders;

24.27 Securities brokerage;

24.28 Telecommunications companies

24.29 Utility companies

24.30 Securities Exchange

25**.** A "Relevant Financial Transaction" for the purposes of the Guide involves the provision of the foregoing services.

WHEN DOES THE GUIDE APPLY TO A TRANSACTION

The Business Relationship

26**.** The Guidelines will apply to a Relevant Financial Transaction involving an arrangement between two or more parties when at least one of the parties is acting in the course of business. It also applies to the formation of a "business relationship" the purpose of which is to agree an arrangement to facilitate the carrying out of Relevant Financial Transactions between the parties concerned on a frequent, habitual or regular basis and when the aggregate payment in respect of transactions in the course of the arrangement is either uncalculated or is incapable of being ascertained at the time when the relationship is formed. Care and diligence shall be exercised in assessing whether or not the Guidelines apply to business undertaken.

27**.** An Isolated Transaction should be treated as any other transaction. Where circumstances are questionable and unexplained and if money laundering is suspected**,** identity should be verified and a report made in accordance with Section IX of this Guide.

SECTION IV: THE MONEY LAUNDERING LEGISLATION

OUTLINE OF THE OFFENCES

28. The legislation specifically relating to money laundering is contained in the Money Laundering Prevention Act, No 8 of 2011, and the Proceeds of Crime Act, No 4 of 1993 in Dominica. **See Appendix 1 for definitions and offences.**

OUTLINE OF THE REPORTING REQUIREMENTS

29**.** All suspicious transactions shall be promptly reported to the Financial Intelligence Unit For that purpose suspicious transactions reporting forms (STRs) will be provided by the Financial Intelligence Unit. The STRs should be filed immediately after a suspicion is formed and should not under any circumstances exceed 5 calendar days. For cases involving isolated transactions and declined business that raise suspicion, the FSP should inform the Financial

Intelligence Unit immediately by telephone or other means before filing a formal report. **See Appendix 2 for reporting form.**

TIPPING OFF OFFENCES

30. Money Laundering Prevention Act, 8 of 2011:

Section ***6(1)*** ***A person who has reasonable grounds to believe that an investigation into money laundering has been, is being, or is about to be made shall not prejudice the investigation by divulging the fact to another person.***

Section ***6(2)*** ***A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding two hundred and fifty thousand dollars, and to imprisonment for a term not exceeding five years.***

SECTION V: INTERNAL CONTROLS AND PROCEDURES

GENERALLY

Written Systems of Internal Controls

31. All financial services providers shall establish and maintain a written and effective system of internal controls which provides appropriate policies, processes and procedures for detecting and preventing activities of money laundering and terrorist financing. The written system of internal controls established shall be framed in a way that would enable the financial services provider to effectively conduct an assessment of the risks that a business relationship or one-off transaction may pose with respect to money laundering and terrorist financing; and be appropriate to the circumstances of the business relationship or one-off transaction, having regard to the degree of risks assessed.

A financial services provider written AML/CFT policies and procedures (systems of internal control) **MUST** be written, approved by senior management and or the Board of Directors of the financial services provider, and **approved by the Financial Services Unit.**

32. Procedures should be established to obtain and maintain appropriate evidence of client identity, and of financial transactions. For the purposes of this guide, there is no distinction between a client and a customer. For convenience the term "client" is used in the Guidelines to include both. Adequate records of client identity and the transactions involved should be maintained in such a manner to assist, if necessary, in the investigation and prosecution of

criminal offences, according to Section 8 of the Money Laundering Prevention Regulations, S.R.O. 4 of 2013.

The provisions in the Guidelines relating to the verification of identity, which apply to Relevant Financial Transactions and new business relationships, apply to those conducted or established after the introduction of the Guidelines. Good industry practice requires, however, that Financial Services Providers should take reasonable steps to ascertain whether further due diligence steps are necessary in relation to existing clients and relationships established prior to the Guidelines coming into effect. As a clear policy, Financial Services Providers should conduct a risk assessment of all of their existing clients and to conduct a complete review of all high risk clients within twelve months. Thereafter, know your customer files for lower risk categories should be reviewed whenever there is client contact. Financial Services Providers are also expected to implement a system of periodic review of customer account activity and reporting of unusual or suspicious transactions.

33**.** Arrangements should provide for the screening of prospective employees on recruitment. It is essential that a full CV is held and that references are obtained directly from former employers. Where any gaps in the employment history exist they should be investigated. Where an employee claims a qualification they should be asked to provide the evidence of this and copies should be retained on the staff file. Similarly, they should provide evidence of previous training through certificates, and where these are not available, training details should lend themselves to easy verification. **It is important to *KNOW YOUR EMPLOYEES.***

All employees should have permanent access to the Guidelines and any regulations for the prevention and detection of money laundering and they should undergo refresher training annually. Procedures should also be adopted to monitor staff compliance with the Guidelines, applicable regulations, policies, internal controls and procedures relating to money laundering. All staff should maintain their own training log which should be reviewed by the MLCO annually.

Compliance Officer and Reporting

34**.** Internal procedures should be put in place for the reporting of suspicious transactions to senior management or a staff designated as the Compliance Officer. Once the member of staff has passed on his suspicions to a senior member of staff or the Compliance Officer, the member of staff has met his responsibility and will be protected from action.

The duty to appoint a Compliance Officer is outlined in section 18 of the Anti-Money Laundering and Suppression of the Financing of Terrorism Code of Practice S.R.O. 10 of 2014, which cross references regulation 5 of the Money Laundering (Prevention) Regulations S.R.O. No. 5 of 2013; the responsibilities of which are outlined at regulation 5 (2) of the above-cited Money Laundering (Prevention) Regulation.

Anyone considered for appointment or designated by a financial service provider to the position of Compliance or Deputy Compliance Officer, MUST first be approved by the Financial Services Unit.

The Compliance Officer should be able to independently determine whether or not a report should be made to the Financial Intelligence Unit if transactions are deemed to be suspicious.

The Compliance Officer should, where appropriate, be an integral part of the organizational structure of Financial Services Providers and should be capable of ascertaining whether a report should be made to the Financial Intelligence Unit.

Appointment of a Deputy Money Laundering Compliance Officer
A financial service provider may appoint a deputy MLCO whose responsibility it will be to cover for the absence of the MLCO. There must be cover for the MLCO at all times to ensure that there is never any absence of the oversight of a financial service provider's AML/CFT policies and procedures and in particular, the detection, investigation and reporting STR's. If an MLCO is in some doubt over reporting a particular transaction he should err on the side of caution and report it.

35. Users of the SWIFT[1] system for telegraphic fund transfers should include the names, addresses and/or account numbers of the ordering and beneficiary clients in all SWIFT MT 100 messages. This is also a specific requirement under FATF Special Resolution 7 re electronic payments.

36**.** Financial Services Providers should have specific policies and procedures for the acceptance of cash for the account of clients. **This is particularly important for offshore business where cash should not constitute a significant form of conducting financial transactions**.

37**.** Financial Services Providers that issue debit and credit cards should have policies and procedures for monitoring account activity and for detecting and reporting unusual or suspicious activity.

GROUP POLICIES

38**.** Many Financial Services Providers in Dominica are branches or subsidiaries of foreign entities, which may require adherence to a group policy in respect of money laundering prevention and detection procedures. They can, of course, adhere to those policies but must ensure that those in respect of verification of identity, record keeping, detection, reporting of suspicious activity and training, do not fall below the standard required by Dominica's anti-money laundering legislation, regulations and this set of Guidelines. Where appropriate, it is important that such group procedures allow for the transfer of identification and other relevant

[1] Society for Worldwide Interbank Financial Telecommunication

documentation to them promptly on request. Consideration should be given to legal and other restrictions on the transfer of information when deciding on the domicile for such information.

39. Where a Financial Services Provider itself has an overseas branch, subsidiary or affiliate over which control can be exercised, it is recommended that a group policy be established to the effect that they should observe verification of identity and record keeping to a standard which is at least that required under Dominica's legislation. It is recognised that reporting procedures and the provisions of money laundering legislation in the jurisdiction in which the branch, subsidiary or associate carries on business must be adhered to in accordance with local laws.

40. When a group policy is operated a Financial Services Provider must be in a position to make a report in accordance with the Guidelines. In certain circumstances, it is possible that a group may make a disclosure in more than one jurisdiction. If this occurs, particular attention should be paid to the tipping off provisions within the law.

SECTION VI: PROCEDURES FOR CLIENT VERIFICATION

INTRODUCTION

41. As a general rule, a business relationship should not be established unless and until evidence of identity of a prospective client is satisfactorily established. In the case of insurance companies or intermediaries, customer due diligence procedures should include procedures to :

- Identify the underlying principal(s) or beneficial owner of the customer, and take reasonable measures to verify the identity of the underlying principal(s) or beneficial owner such that the insurance company or intermediary is satisfied that it knows who the underlying principal(s) or beneficial owner is.
- Identify and verify the identity of the beneficiary of the insurance contract at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.
- Obtain appropriate additional information to understand the customer's circumstances and business, including the purpose and the expected nature of the relationship. Relevant Customer Due Diligence information should be periodically updated as part of the risk assessment process.

If a prospective client refuses or is unable to produce any of the information requested, the relationship should not be established.. Likewise, if follow-up information is requested and is not forthcoming, any relationship already initiated should be discontinued, and any funds held to the order of the prospective client should be returned to the exact source from which they came and not to a third party. If failure to complete identification raises suspicion, a report should be made to and guidance sought from the Financial Intelligence Unit as to how to proceed.

42. If the Financial Services Provider is not satisfied that the transaction in which it is or may be involved is bona fide, it should make further enquiries and decide whether it is appropriate to continue the relationship. In circumstances in which the relationship is discontinued, funds held to the order of the prospective client should be returned as in paragraph 41 above. If failure to complete identification raises suspicion or if money laundering is suspected, a report should be made to the Financial Intelligence Unit and its guidance sought as to how to proceed.

43. Financial Services Providers should ensure that all relevant staff are familiar with and apply procedures to verify and adequately document the true identity of clients. For these purposes, identity will usually include a current address or place of business, and a reliable identity document such as a passport.

44. When Reliance may be Placed on the Procedures of Introducing Intermediaries

As a general rule, Financial Services Providers are responsible for obtaining documentary evidence of identity of all clients as required by this Guide (or other applicable laws and regulations).

However, reliance may be placed on the due diligence procedures of others only where the client is introduced by a regulated Financial Institution which is part of the Corporate Group (e.g. a branch, subsidiary, parent or affiliate of the Financial Services Provider) which has conducted client verification procedures substantially in accordance with this Guide, and where written confirmation is received from the Financial Institution that documentary evidence of identity has been obtained and will be supplied before establishing the relationship (e.g. before funds are transferred in or out of an account).

Financial Services Providers should satisfy themselves that copies of identification data and other CDD documentation mentioned in this guide will be made available from the introducing financial institution upon request without delay.

If the introducing Financial Institution fails to provide adequate evidence of identity, the relationship shall be discontinued unless other appropriate steps are taken to verify identity. Where the relationship is discontinued and funds are held to the order of the client, the funds shall be returned and only to the source from which they came and not to a third party. If failure to complete verification of identity itself raises a suspicion of money laundering, a report should be made to and guidance sought from the Financial Intelligence Unit as to how to proceed.

Financial Services Providers should be aware that they have ultimate responsibility for CDD and verification even where reliance is placed on the intermediary for conducting these measures.

45. Procedures should be established to obtain information to distinguish those cases in which a business relationship is commenced or a Relevant Financial Transaction is conducted with a person acting on behalf of others. If it is established that a client is acting on behalf of another (i.e. he is an Intermediary Client) the procedures in paragraphs 80 – 84 et seq. below should be applied. For example, in the case of a mutual fund KYC should be conducted on the directors of the fund and the promoter.

46. There may be other cases in which the Financial Services Provider may regard a person as his client although he may have no contractual relationship with him. For example, a mutual fund administrator/manager will often regard the promoter or sponsor of the fund as his client. In such cases reasonable business procedures will be necessary to decide who should be included in the category of client for the purposes of verification of identity.

47. Particular care should be taken in cases of clients (whether companies, trusts or otherwise) which conduct no commercial operations in the country in which their registered office is located or when control is exercised through nominee or shell companies. Special procedures should also be developed for dealing with corporate clients that issue Bearer Shares to ensure that the beneficial ownership is always known to the Financial Services Providers.

48. Financial Services Providers should not do business with persons using obviously fictitious names and should not keep anonymous accounts, or accounts where it is impossible or difficult to identify the client. This is prohibited under Section 10 of the Offshore Banking (Amendment) Act, No. 16 of 2000, and is also prohibited in the Banking Act.

49. When appropriate and practicable, a prospective client should be interviewed, but in such cases procedures for obtaining evidence of identification should still be followed. Information relating to occupations or business activities and source of funds should be obtained.

Translation of Documents: Where a financial services provider receives a document in a foreign language he should ensure that the document is adequately translated with a record held on the client file.

Isolated Transactions

50. Verification of identity will be needed in the case of an Isolated Transaction. If, for example, the transaction is merely one to exchange foreign currency, then it would be sufficient to validate identity using the original passport plus the credit card or travellers cheque being presented for payment. If, however, the circumstances surrounding the proposed Isolated Transaction appear to the Financial Services Provider to be unusual or questionable, it may be necessary to make more detailed enquiries. Depending on the result of such enquiries, if money laundering is known or suspected, the Financial Services Provider should make a report in line with Section IX of this Guidelines and Section 19 of the Money Laundering

(Prevention) Act, No. 8 of 2011, irrespective of the size of the transaction using the STR form as scheduled in the Money Laundering Prevention Regulations. Guidance from the Financial Intelligence Unit should be sought as to how to proceed.
The following should be obtained for isolated transactions:

- The customer's background.
- His country of origin and residence.
- His public or high profile position.
- Any linked accounts.
- The nature and location of his personal or business activities.
- The volume of transaction, or transactions involving large amounts.
- His business partners.

EXEMPTED CATEGORIES

Exempted Clients

51. Documentary evidence of identity will not normally be required if the prospective client:

51.1 is a central or local government, statutory body or agency of government unless money laundering or other illegality is known or suspected;

51.2 is an onshore financial institution regulated and supervised by the Eastern Caribbean Central Bank (ECCB);

51.3 is a broker member of the OECS Stock Exchange as defined in the OECS Stock Exchange membership rules (or other similar document);

51.4 is a regulated and supervised bank in a country where the Central Bank has fully effective regulatory jurisdiction and where the Country is not a high risk country.

51.5 is an existing client prior to the issue of the Guide and the Money Laundering (Prevention) Act. In such cases, the Financial Services Provider shall reassess whether or not there is a need for further information about the identity of the client, the nature of his business, the source of funds or the address he has given; based upon a written risk assessment model which must be available for review by the FSU. In cases where the risk is assessed as high full due diligence is required before the transaction is entered into. Best practice would be to obtain due diligence for all other clients at the next client contact.

51.6 is a pension fund for a professional association, trade union. Satisfactory evidence that the fund falls within this category may be provided by a copy of a certificate of registration, approval or regulation by a government, regulatory or fiscal authority in the jurisdiction in which the fund is established. In the absence of such certificate, Financial Services Providers are recommended to obtain the names and addresses of the trustees of the fund (if a trust) or otherwise of those empowered to take decisions in respect of it.

52**.** If reliance is to be placed on the fact that a client is an exempted client, the Financial Services Provider should satisfy himself appropriately that he does in fact fall within this category. The Financial Services Provider should record the basis upon which he is so satisfied.

Payment on an Account in a Financial Institution in Dominica.

53**.** When a Relevant Financial Transaction involves one-off payment by the client and he does so by remitting funds from an account in a regulated Financial Institution in Dominica, it may be unnecessary to take any further steps to verify client identity if the Financial Services Provider has evidence identifying the branch or office of the regulated Financial Institution and verifying that the account is in the name of the client. Thus, for example, it may be reasonable to take no further steps to verify identity when such payment is made by cheque or electronically and sent either by mail or electronically from an account (or joint account) in the client's name at a bank in a country that sufficiently applies the FATF 40 + 9 recommendations (see *schedule of appropriately approved jurisdictions*). This does not remove the obligation to issue an STR if money laundering or terrorist financing is suspected.

When business is placed over the telephone or, for example, by mail-shot and payment is made in this way, a record should usually be retained indicating how the transaction arose in addition to a record of the relevant branch or office and the account name and number and the clients core due diligence information such as name, address, country of origin and likely activity. It is important that the information retained be sufficient for initiating a money laundering investigation should the need arise. Also that sufficient information is retained so that funds can be remitted back to the same account from which they were originally provided. A minimum retention period of seven years is required under Section 49 of the Proceeds of Crime Act, and Section 16 (1) of the Money Laundering Prevention Act, No. 8 of 2011.

TIMING OF VERIFICATION

54**.** It will not always be possible to obtain satisfactory verification of evidence immediately upon contact by a prospective client. In such circumstances evidence should be obtained as soon as reasonably practicable. Usually verification procedures should be substantially completed before the business relationship is established but there may be circumstances in which it is acceptable to proceed pending completion of those procedures. It would not be appropriate to complete settlement of the Relevant Financial Transaction, to transfer or pay any money out to a third party, or dispatch documents of title before adequate verification evidence is obtained.

SPECIFIC VERIFICATION PROCEDURES WHEN NO EXEMPTION APPLIES

55**.** In all other cases the best available documentary evidence of identity should be obtained. These should comprise copies of documents, which are difficult to forge or obtain illegally, and are easy and inexpensive to verify. The following paragraphs reflect reasonable business procedures but they are not exclusive. It is recognised that other means of identification may be reasonable depending on the circumstances of the client, the laws of his business location or the nature of the business undertaken. For example, when dealing with the elderly, the infirmed and minors, it may be difficult to obtain identification documents since they may not exist or may be difficult to brought in person. These groups may be considered as low risk and unless the analysis of transactions reveals anomalies a risk-focused and flexible approach should be adopted here. Procedures used for non-face-to- face customers may be used if they are unable to come in person. Examples of such procedures include certification of documentation presented and independent contact of customer by the bank. FSPs should also obtain identification documents from the parents/guardians that introduce or consent to the opening of accounts for minors, in addition to those of the minors.

INDIVIDUALS

Scope

56**.** The procedures described below shall apply to the opening of accounts or initiation of a business relationship carried out in all the branches or offices of the Financial Services Provider. They involve accounts and transactions involving receipt, delivery or transfer of funds of any kind including, but not limited to, deposit accounts, savings, investments, trusts, mandates, commissions, safe deposit boxes and the granting of loan, credit or guarantee services of whatever kind, except for cases set forth in the Exempted Categories.

Interviews

57**.** Where appropriate, interviews should be conducted to "*know the customers"*, understand their moral qualities, their professional, trade or business goals and characteristics,

in accordance with practices and customs of the business line or profession. Always ask why the customer is considering opening an account in Dominica.

References

58**.** It is important to obtain references from banks and other professional firms. These references should be requested by the Financial Services Provider and be received directly from the banks and other firms providing such references. **Under no circumstances should a letter of reference be accepted from the new customer as it could be forged or altered. Verify bank reference and document confirmations.**

Identifying the Client

59. Identification requirements shall be obtained and recorded for the client depending on the nationality of the prospective customer. The applicant for business or representative shall be required to provide an official valid form of identification, with photograph, signature and if applicable, an address. Identification information to be obtained and documented include, among others:

59.1 Passport or national identity card. When passports are used, ask whether multiple passports have been issued, e.g. those acquired under economic citizenship programmes. There are official Interpol Passport Guides which list the most popular passports and incorporate details of the validations which are incorporated within the original documents. Black and white copies of the passport should be held on file. This helps the financial services provider in the context of having both a photo and a signature of the client on file for future business transactions and as an audit trail of maintaining compliance with the money laundering legislation and guidance. It may also help the authorities in tracking down someone subsequently involved in illegal activity and facilitate criminal investigations and prosecutions.

Driver's licence, social security card, military service card, voting card, major credit card with photograph, border/immigration card/form, etc. may also be used as supplementary identification sources. Please note that passports and other cards are **NOT** fool proof and are sometimes forged or counterfeited. Documents that are easily obtained should be accepted uncritically and may be used only as supplementary documentation (e.g. employer identity cards, credit cards, and social security cards.)

If the passport or national identity card is not presented in person, a certified copy should be requested.

Certification of Identification Documents

A certifier must be a suitable person, such as a lawyer, accountant, director or manger of a regulated institution, a notary public, a member of the judiciary, a senior civil servant, a consular official or a serving police officer.

The certifier should sign and date the copy document (printing his name clearly in capitals below), state that it is a true copy of the original, and clearly indicate his position or capacity on it. If a covering letter is used it is important to establish the document to which the letter refers.

Where certified documents are accepted it is up to the FINANCIAL SERVICE PROVIDER to satisfy himself that the certifier is appropriate.

59.2 Date and Place of Birth and Nationality(ies)

59.3 Signature cards completed and signed;

59.4 Account opening forms completed and signed;

59.5 Place and description of the customer's principal line of business;

59.6 Customer's residence;

59.7 Telephone and fax numbers, residence and business;

59.8 Clients Occupation, when appropriate, visit the place of business to verify that the business actually exists and coincides with the information provided by the customer; and provides an indication of expected account turnover and activity.

59.9 Source of funds and expected account activity is extremely important to establish customer profile. Proposals to make large deposits of cash or monetary instruments, or wire transfers inconsistent with the customer's business or profession should be queried;

59.10 A declaration of source and purpose of funds should be completed and signed. This should provide for: business or professional activity of the customer, purpose of the account, source of funds, use of funds, expected number of transactions per week/month/quarter as appropriate, average amount of transactions per week/month/quarter as appropriate, etc.

59.11 Where necessary, follow-up calls may be made or a letter sent to the customer's residence, place of business or other address given. Disconnected telephones or lack of response warrant further enquiry;

59.12 Where reasonable, check with credit and similar service bureaus for questionable activities by customer;

59.13 If the address is not provided on the piece of identification documentation, or if it does not coincide with the address given in account opening documentation, proof of address may be obtained by requiring any one or more of the following: property tax receipts, utility payment receipts, lease agreement, statement of bank and credit card accounts, letter of employment, etc. No form of proof should be more than six months old.

60**.** Particular care should be taken to obtain adequate documentary evidence of identity in any case where prospective clients deal with the Financial Services Provider by mail or by coupon applications. In such limited and exceptional cases, when it is not practicable to meet an overseas client at the time the relationship or account is established, it may be appropriate for an application for business to be channelled through a reputable source such as a regulated bank in the prospective client's jurisdiction which itself can be relied upon to verify identity in an appropriate and effective way and to provide copies of evidence. A decision to obtain evidence of identity in this manner should only be taken by senior management and properly recorded.

61**.** Where an authorised signatory other than the account holder is to be appointed, the information requested under paragraph 58 and sub-paragraphs 59.1, 59.3, 59.4, 59.5, 59.6 and 59.7 should be obtained and kept on file.

CORPORATE CLIENTS

General

62. Financial Services Providers should recognize that the use of corporate vehicles is attractive to money launderers and should therefore exercise appropriate care. Wherever possible the Financial Service Provider should "lift the corporate veil" in order to find out who is the beneficial owner. When conducting business with companies with bearer shares, if the Financial Services Provider is unable to identify the beneficial owner, then he should not proceed with the relationship. The registered office provider/registered agent/manager of a Dominican company will have obtained relevant information relating to client identity. Financial Services Providers should, however, usually obtain and record the following information:

62.1 full name and address of the company, and name and address of registered agent or company manager (if applicable);

62.2 place of incorporation;

62.3 certified copy of incorporation documents by the issuing Registrar such as: certificate of incorporation and memorandum of understanding and where applicable, certificate of change of name, certificate of good standing, copy of the register of directors and officers. As legal controls and requirements vary between jurisdictions, particular attention may need to be given to the place of origin or domicile of such company or documentation and the background against which it is produced;

62.4 A properly authorised mandate and a copy of the company's resolution to establish the business relationship should also be requested. Powers of attorney or other similar assignment of power can also be used;

62.5 The company should provide evidence of authorisation for all account signatories;

62.6 A statement of source of funds and purpose of the account should be completed and signed. This should also show the expected turnover or volume of activity in the account as for Individuals under sub-paragraph 59.10 above;

62.7 Standard account opening forms should be completed and signed by authorised individuals.

63. It is particularly important to have an understanding of the nature of the business conducted by a company and to be able to identify its directors, shareholders and ultimate beneficial owners.

64. Copies of identification documents should be obtained for at least two directors (if there is more than one) and authorised signatories in accordance with the general procedure for the verification of the identity of individuals.

65. For large corporate accounts, the following should be obtained: annual reports/audited financial Statements for the previous 5 years or from the commencement of operations if less, description and place of principal line(s) of business, list of major business units, suppliers and customers, etc. where appropriate.

Closely Held Companies and Companies Owned by Closely Held Companies

66. In addition to corporate identification requirements outlined under paragraphs 62 – 65 above, where the client is a closely held company[2] the Financial Service Providers should obtain a copy of the register of members or a list of the names and addresses of shareholders holding a controlling beneficial interest. It may also be necessary to obtain identification

[2] May need to define what a closely held company is.

details which would be required of an individual client for individuals who are beneficial owners holding or controlling 5% or more of the issued shares of a company.

67. If the shareholder of the corporate client is a closely held company (or companies), the following information should be obtained:

67.1 information as for individuals regarding ultimate beneficial shareholder(s) as under paragraph 68;

67.2 copies of corporate documents or filings to show that the holding company(s) are in good standing and of good repute. It should be remembered that certificates of good standing represent nothing more than confirmation that the current years fees have been paid over to the companies registry. (If there is any doubt and where practical, it may be necessary to institute a company search or make inquiries of a credit reference or similar agency.) Consideration should be taken of whether the country sufficiently applies the FATF recommendations. Guidance on certification is included in Appendix 13 and guidance on the countries which sufficiently apply the FATF recommendations is included in Appendix 4.

Companies Listed on a Recognised Stock Exchange

68. In cases of a corporate client, which is listed on a recognised stock exchange, or where the shareholder or other intermediate shareholders are companies that are listed on a recognised stock exchange, the following information on the listed companies should be obtained and placed on file:

68.1 Evidence of the listing, including a copy of the company's Annual Report, Bloomberg or Reuters Extract or any other satisfactory current evidence that the company is listed and in good standing.

68.2 A written statement of objectives and purpose for which the company or companies was formed and the source of its funds.

68.3 Verification of identity of each beneficial shareholder holding more than 20% ownership interest in the company.

69. Where the Financial Services Provider is not satisfied as to the bona fides of the listed company(s), identification information such as that listed under paragraphs 62 – 64 may be requested.

Companies Owned by Partnerships

70. In addition to information required under paragraphs 62 – 68 above, where the shareholder or ultimate shareholder of a corporate client is a partnership, the Financial Services Provider should request the following information on the partnership:

70.1 A copy of the partnership agreement;

70.2 Identification information as for Individuals for the controlling partner or partners, particularly of the partner who has the authority to represent the partnership.

Companies That Issue Bearer Instrument e.g. Bearer Shares, Warrants, Notes, Bonds…)

71. In addition to the identification information required under paragraphs 61 – 64, where a company's stock has been issued to bearer (a "bearer stock" company), it would be prudent that the bearer share certificates be held in custody and under the control of the Financial Services Provider. This measure is extremely important to prevent changes in ownership and control of the company (and any assets or liabilities accruing to it) without the Provider's knowledge. In addition, it is important that the Financial Services Provider ascertains whether any beneficial ownership interests or rights attach to the bearer shares. Failure to be in control of bearer shares may result in the Services Provider dealing with anonymous or undesirable customers thereby exposing it to money laundering risk.

72. Where it is not practical for the Financial Services Provider to have physical custody of the bearer shares, there may be circumstances where it may be reasonable to accept that the shares are held by another custodian of good repute, such as a bank that is well known to the Provider. This will only be acceptable where the reputable custodian has given a written undertaking that custody of the bearer shares will not be released, and that no change to any beneficial ownership interests or rights will be effected, without the prior knowledge and consent of the Provider. The Financial Services Provider should ensure that any restrictions on disclosure of information have been duly waived.

PARTNERSHIPS & UNINCORPORATED BUSINESSES

73. In the case of Dominican limited partnerships, the Financial Services Provider should obtain a certified copy of the certificate of registration and a certificate of good standing by the Registrar General. The Financial Services Provider should also obtain, where relevant, information similar to that for corporate clients under paragraph 65.

74. In the case of other unincorporated businesses or partnerships in which, for example, the general partner does not fall within the exempted category set out in this Section, Financial Services Providers should obtain, where relevant:

74.1 evidence of the identity of a majority of the partners, owners or managers, and the authorised signatories, in accordance with the general procedure for the verification of identity of individuals;

74.2 a copy of the mandate from the partnership or unincorporated business authorizing the establishment of the business relationship, and confirmation of any authorised signatories; and

74.3 a copy of the partnership agreement or documents governing the business.

INTERMEDIARY CLIENTS

Clients Acting on Behalf of a Third Party or as a Trustee or Nominee

75. A Financial Services Provider shall identify whether or not a client is acting as an intermediary on behalf of another. If the prospective client is acting on behalf of a third party (and neither is within the category of exempted clients in this Section) it will, as a general rule, be necessary to follow verification procedures and obtain appropriate information in respect of third parties for whom the Intermediary Client will act. If the prospective client is a trustee or nominee, the Financial Services Provider should obtain appropriate identification information in respect of the following:

75.1 the principal for whom a nominee acts;

75.2 the beneficiaries;

75.3 any person on whose instructions or in accordance with whose wishes the trustee or nominee is prepared or accustomed to act;

75.4 the settlor or grantor of a trust;

75.5 the nature of the duties or capacity of the trustee or nominee.

76. It may be necessary to verify the identity of an underlying client even where the Intermediary Client is itself an entity in Dominica to which this Guide applies or falls into the category of acceptable clients. Such cases will normally arise where the Services Provider has doubts about the completeness or availability of identification information on the underlying client. The Services Provider, may however, establish a business relationship with the Intermediate Client with an undertaking that the identification information will be provided within a reasonable period of time and before any transactions are effected on behalf of the underlying client.

77. Documentary evidence of identity of an underlying client will not be necessary if it falls into the category of exempted clients in this Guide. However, proof of the exempted status of the underlying client should be obtained and placed on file.

78. For lawyers, accountants and other professional intermediaries legal privilege would not apply where a client engages financial transactions such as the buying and selling of

real estate; management of client money, securities, or other assets; management of bank, savings or other securities; creation, operation or management of legal persons or arrangements and buying and selling of business entities; and organisation of contributions for the creation, operation or management of companies. In these circumstances, documentary evidence of the identity of an underlying client will be necessary.

79. In other circumstances, the Financial Services Provider should not proceed with the relationship or transaction.

PROCEDURES SPECIFIC TO TRUSTEES

80. A trustee should verify the identity of a settlor/grantor or any person adding assets to the trust in accordance with the procedures relating to the verification of identity of clients. In particular, the trustee should obtain the following minimum information:

80.1 **Settlor or any person transferring assets to the trust:** name, address, business, trade or occupation, and other information in accordance with the procedures relating to the verification of client identity outlined in this Guide;

80.2 **Beneficiaries:** name, address and other identification information such as passport number, etc;

80.3 **Protector:** name address, business occupation and any relationship to the settlor;

80.4 **Purpose and nature of trust:** a statement of the true purpose of the trust being established, even where it is a purpose or charitable trust (e.g. STAR trust);

80.5 **Source of funds:** identify and record the source(s) of funds settled on the trust and the expected level of funds so settled;

80.6 **Bank references:** this may be part of the identification requirements for the settlor under 80.1 above.

81. The trustee should also ensure that payments from the trust are authorised and made in accordance with its terms.

PROVISION OF CUSTODIAN SERVICES AND SAFETY DEPOSIT BOXES

82. For those Financial Services Providers acting as custodians or otherwise offering safe-keeping services, particular precautions need to be taken in relation to requests to hold boxes, parcels and sealed envelops in safe custody. In such cases, the client identification procedures set out in this Guide should be followed. Bank employees should not act as agents for clients in transferring anything in or out of safety deposit boxes.

INTERNET AND CYBER-BUSINESS

83. Any Financial Services Provider offering services over the Internet should implement procedures to verify the identity of its clients. Care should be taken to ensure that the same supporting documentation is obtained from Internet customers as for other customers particularly where face-to-face verification is not practical.

84. In view of the additional risks of conducting business over the Internet, Financial Services Providers should monitor activity in customer accounts opened on the Internet on a regular basis.

HIGH RISK JURISDICTIONS AND INDIVIDUALS

85. From time to time, the authorities or management may determine that because a high incidence of money laundering is associated with persons from certain countries or regions, additional precautions are required to safeguard against use of accounts or other facilities by such persons or their representatives. Under these circumstances, it may be necessary to request a letter of reference (confirmed), in addition to the other identification requirements, from a regulated bank which is not from the countries or regions in question.

Whilst there is not a preclusion from conducting business which Politically Exposed Persons (PEPs) there is a need to be much more vigilant with regard to these relationships.

FSPs should have risk management systems to determine whether the customer or beneficial owner is a PEP by checking both new and existing clients against the international watch lists which are published by the ECCB, the United Kingdom's Financial Services Authority, the FIU, the United Nations and United States Treasury Office of Foreign Assets Control (OFAC). Financial Institutions may also access electronic databases from commercial providers who provide international name checking services.

Employees should be required to obtain senior management approval for establishing business relationships with PEPs. If the customer or beneficiary is found to be or becomes a PEP after the start of a business relationship the FSP should obtain senior management approval for the continuation of the relationship and should conduct ongoing enhanced monitoring of it. FSPs should take reasonable measures to establish the source or wealth and source of funds of customers and beneficial owners identified as PEPs.

FSPs can also be exposed to additional risk from non PEP customers if they are not in regular contact. One typical situation is the "hold mail" client. Whilst there may be perfectly legitimate reasons for operating the account in this manner it should be the subject of enhanced

ongoing monitoring. Enhanced monitoring would entail more careful scrutiny of transactions and ongoing CDD on the customer and beneficial owners.

As well as individuals there are countries which may require much higher levels of vigilance due to their being home to significant corruption and / or other illegal activity (Abacha and Nigerian letters would be a good examples). Please see Appendix 12 for information sources which may be used in developing risk management systems.

SECTION VII: STAFF TRAINING AND EDUCATION

INTRODUCTION

86. All staff, particularly those dealing with client accounts, assets, accounting and record keeping, should be familiarized with the risk of inadvertent, and intentional, involvement in money laundering. Upon hiring and routinely thereafter, measures should be taken to ensure that they are aware of this Guidelines and any relevant guidelines and procedures relating to the avoidance, recognition and reporting of suspected money laundering activities. Senior management and staff responsible for internal audit and compliance should be particularly familiar with all the relevant laws and regulations pertaining to money laundering. Each Financial Services Provider will decide for itself how to meet the training needs of its officers and employees in accordance with its particular commercial and other requirements.

87. Vigilance to avoid and detect involvement in money laundering should be a continuous effort throughout the organization or business unit at all levels of staff including where appropriate clerical, secretarial and administrative staff. The extent of training necessary will depend on the nature and scope of the business conducted and the size of operations.

88. Staff compliance with the guide, laws, regulations and internal policies should be monitored on a regular basis. Special attention should be given to compliance with procedures for establishing and maintaining appropriate records. Where appropriate, a strong and independent compliance and internal audit function should be established to monitor and report on adherence to these requirements. For larger financial services providers, consideration might also be given to separating the role and function of the Compliance Officer for all regulatory compliance and the officer responsible for reporting suspected money laundering issues the MLRO (money laundering reporting officer). This does not mean that both roles could not be fulfilled by the same single individual in smaller financial services providers.

89. Where one has been appointed, the Money Laundering Compliance Officer shall undergo in-depth training concerning all aspects of the anti-money laundering laws, regulations, guidelines, policies and procedures. In addition, extensive and continuing

instruction on the validation and reporting of suspicious transactions and interaction with investigation authorities will be required.

90. It is very important that staff be made aware of the legal, reputation and financial risk money laundering poses to the Financial Services Provider and to themselves. Consequently, training procedures should provide for guidance on how to avoid tipping off clients who may be the subject of a suspicious activity report or investigation. It is important to stress that even delaying response to or declining to act for an affected client might make them aware of something that could amount to tipping off. The penalty for tipping off on conviction is a fine not exceeding five hundred thousand dollars and to imprisonment for a term not exceeding five years.

91. Financial Services Providers are encouraged to use national and regional sources of anti-money laundering training and where practical, incorporate the use of videos, computers, the Internet and other media in their training programmes.

REPORTING PROCEDURES

92. Staff should be aware of the internal reporting procedures and policies to be followed. They should also have access to advice on compliance with this Guidelines and reporting procedures.

NEW EMPLOYEES

93. It is extremely important to ***know your employees.*** Proper screening procedures should be adopted to ensure that only honest and law-abiding persons are employed.

94 All employees should at the commencement of employment be made aware of what constitutes money laundering and their potential personal liability under the money laundering legislation. Special attention should be given in training to combating and preventing money laundering.

95. They should have the Money Laundering Compliance Officer (where one has been appointed) identified to them and should be trained in reporting procedures.

SECTION VIII: RECORD KEEPING

GENERALLY

96. Appropriate records should be maintained to establish an audit trail that can be used to carry out criminal investigations. What is appropriate requires a balance between normal commercial considerations and the needs of investigating authorities. Legal advice may be sought on the type of records and period of retention to satisfy legal, regulatory and investigative requirements. These should usually therefore include evidence of client

identities and addresses, and sufficient details of accounts and transactions, and should at least meet the requirements of Section 49 of the Proceeds of Crime Act, and the requirements of the Money Laundering (Prevention) Regulations.

97. The documentation should be prepared and stored (whether by original documents, copies or on microfiche or other accessible computerized form) in such a way that they are accessible within a reasonable time and available to comply with any court orders regarding disclosure of information, restraint or confiscation of assets.

98. It is recommended that, when practicable, appropriate evidence of client identification, account opening or new business documentation and adequate records identifying and describing financial transactions should be kept for a period of 7 years following the closure of an account, the end of the transaction or the termination of the business relationship.

99. Where there has been a report of a suspicious transaction, or the Financial Services Provider is aware of a continuing investigation into money laundering relating to a client or a transaction, records relating to the transaction or the client should be retained until confirmation is received that the matter has been concluded. Legal advice and guidance from the Financial Intelligence Unit may be sought in such cases.

100. The Financial Services Provider should maintain a detailed record/register of all suspicious activity reported to the Financial Intelligence Unit and of all enquiries made to it by the authorities relating to money laundering.

Transaction Records

Financial Institutions should already hold comprehensive records of transactions not all of which will be relevant from an anti-money laundering point of view. The following sets out the elements that should be held to satisfy the regulations:

- The volume of funds flowing through the account / turnover of client company;
- The source of the funds;
- The form in which the funds are transacted (cash or cheque);
- The identity of the person undertaking the transaction;
- The destination of the funds;
- The form of instruction and authority;
- The name and address of the counterparty;
- The security dealt in including price and size;
- The account details from which the funds were paid;
- The form and destination of payment made by the business to the customer;

- Whether the investments were held in safe custody by the business or sent to the customer or to another part on his order, and if so to what address;
- Activities of the client company.

Training Records

In order to provide an audit trail of staff training for the FSU, Financial Institutions should maintain the following records:

- Details of the content of training provided;
- The names of the staff attending the training;
- The date on which the training was delivered;
- The results of any testing carried out to measure staff's understanding.

GROUP RECORDS

101. Subject to legal provisions relating to confidentiality and disclosure of information, there may be circumstances where records may be stored centrally or outside of the country. In such cases, it is the responsibility of the Financial Services Provider to ensure that appropriate records are maintained and can be retrieved promptly on request. Such arrangements should provide for gateways to restrictions on disclosure and transfer of information.

SECTION IX: RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

102. When there is suspicion that the source of funds may be criminal or that a client may be involved in criminal activity, Financial Services Providers should follow established procedures for assessing the evidence and determining their course of action. Depending on the nature of the suspicion, they must decide whether or not they can continue the business relationship, they should subject it to particular scrutiny or undertake further investigation. In any event, where there is reasonable suspicion that money laundering is about to occur, is occurring or has occurred, a report shall be made to the Financial Intelligence Unit as required under law.

103. What may be suspicious will depend upon the nature of the relationship and the transaction and the particular circumstances. There is no one test that can be applied to determine what constitutes a suspicious transaction but an understanding of the client's business and adequate record keeping will facilitate the assessment. Unsatisfactory explanation or lack of commercial rationale, unusual patterns of transactions and inconsistency with the client's known business may be indicative of a transaction or a series of transactions should be subjected to particular scrutiny.

104. Financial Services Providers should have internal procedures to ensure suspicions about the source of funds, transactions or patterns of transactions are reported the Money Laundering Compliance Officer. The compliance officer must be of sufficient seniority to have access to information, systems and decision makers in order to evaluate whether a report should be made. All staff should be aware of the importance of cooperation with the compliance officer to whom access should be readily available. The Financial Services Provider should maintain a central file of all internal suspicious transaction reports, those that are not filed with the Financial Intelligence Unit should have a signed statement by the MLCO explaining why the suspicious transaction report was not filed with the Financial Intelligence Unit. If a FINANCIAL SERVICE PROVIDER is approached to enter into a transaction of which they are suspicious and decline to do it may be that the client will try to conduct this business elsewhere. If the second FINANCIAL SERVICE PROVIDER is not as careful they may do business which could harm both them and Dominica. If the authorities have been warned they may be able to prevent other Financial Institutions being involved and may be able to prevent a criminal activity.

Reporting Declined Business

There will be many reasons why a Financial Service Provider might decide to decline business or not to enter into a specific transaction. On occasions this will be because the Financial Service Provider either knows or suspects it might be criminal in intent or origin, complex or large.

In such circumstances even though no business connection exists a report should be made to the Financial Intelligence Unit. This will allow the Financial Intelligence Unit to form a picture of any money laundering threats to Dominica and in the longer term may discourage launderers from trying to place criminal business in Dominica in future.

105. A record should be kept of reports made by employees the Compliance Officer, as well as of reports made by the Financial Services Provider to the Financial Intelligence Unit.

106. In the event that a Financial Services Provider declines to accept business from a potential client or to follow a request or mandate because of money laundering suspicion, a report should be made to the Financial Intelligence Unit. Financial Services Providers must be mindful of cooperation with criminal investigations and should,

where practicable, seek and maintain evidence of identity and other relevant information in such cases.

107. In the event of a report being made to the Financial Intelligence Unit, staff should be aware of the dangers of impeding or prejudicing an investigation into money laundering by wittingly or unwittingly tipping off the client or others. The potential for corporate and/or personal legal liability to them should be clearly communicated.

108 A report of a suspicious transaction or activity should be directed to:

The Director
Financial Intelligence Unit
47 Field's Lane
Roseau
Commonwealth of Dominica

Telephone: (767)-266-3349/3348/4145/4146/3084
Facsimile: (767)-440-0373
E-mail: fiu@dominica.gov.dm
Website: www.fiu.gov.dm

109. A standard form for reporting suspicious transactions is included in Appendix 2. It should be remembered that sufficient detail of the client identity and the relevant transaction(s) should be included to enable the authorities to take all necessary steps to investigate.

110. Financial Services Providers are encouraged to maintain regular contact with the Financial Intelligence Unit and to seek general guidance as to the nature of transactions or activities that should or should not be reported.

111. Financial Services Providers will wish to cooperate fully with law enforcement authorities to the extent that they are permitted and/or required by law. If uncertain as to its legal obligations, legal advice may be sought.

APPENDIX 1

GLOSSARY OF RELEVANT DEFINITIONS

Financial Institutions

Reference is made in the Guide to Financial Institutions particularly in the context of due diligence procedures necessary when a prospective client is introduced. In this context, Financial Institutions refer not only to banks but also to non-bank financial institutions, as listed in Part I of the schedule to the Money Laundering (Prevention) Act.

Isolated Transactions

. An "Isolated Transaction" means:

A transaction carried out other than in the course of an established business relationship, for example, a single foreign currency transaction for a customer who does not have an account at the bank concerned constitutes an "isolated transaction"; and

the payment made by or to a person if the transaction is below EC$13,000 (or its equivalent in other currency) unless the payment is one of a series of transactions carried out within three months which are or appear to be linked and in which the aggregate payment exceeds EC$13,000 (or its equivalent in other currency).

Legal Privilege and Legal Professional Secrecy

Legal professional privilege or legal professional secrecy would cover information lawyers, notaries, accountants, or other independent legal professionals receive from or obtain through one of their clients in the course of ascertaining the legal position of their client; in performing

their task of defending or representing the client; or concerning judicial, administrative, arbitration of mediation proceedings.

Money Laundering:

According to Section 2(1) of the Money Laundering (Prevention) Act, No. 8 of 2011, "***money laundering***" means conduct which constitutes an offence under Section 3(1).

Section 3(1) states:
"***A person who -***
(a) receives, possesses, manages or invests;
(b) conceals or disguises;
(c) converts or transfers;
(d) disposes of , brings into or takes out of Dominica; or
(e) engages in a transaction which involves,

property that is the proceeds of crime, knowing or believing the property to be proceeds of crime, commits an offence."
And "proceeds of crime" means any property derived or obtained through the commission of an indictable or hybrid offence whether committed in Dominica or elsewhere.

THIS DEFINITION ALLOWS FOR THE CRIME OF MONEY LAUNDERING TO INCLUDE THE PROCEEDS OF COMMERCIAL FRAUD ETC. AND NOT JUST THE PROCEEDS OF DRUG RELATED CRIME.

Reporting Requirements:

(1) A financial institution or person carrying on a scheduled business shall pay attention to -

i. all complex, unusual or large business transactions, whether completed or not;

ii. all unusual patterns of transactions;

iii. relations and transactions with persons, including business and other financial institutions, from countries that have not adopted a comprehensive anti money laundering legislation.

(2) Upon reasonable suspicion that the transaction described in subsection (1) could constitute or be related to money laundering, a financial institutions or person carrying on a scheduled business shall promptly report the suspicious transactions to the Authority.

(3) A financial institution or person carrying on a scheduled business, shall not notify any person, other than a court, competent authority or other person authorised by law, that information has been requested by or furnished to a court or the Authority.

(4) When the report referred to in subsection (2) is made in good faith, the financial institution or person carrying on a scheduled business and its employees, staff, directors, owners or other representatives as authorised by law shall be exempted from criminal, civil or administrative liability, as the case may be, for complying with this section or for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, regardless of the result of the communication.

(5) A criminal offence is committed by a financial institution or its employees, staff, directors, owners or other authorised representatives or a person carrying on a scheduled business who, acting as such, wilfully fail to comply with the obligations in this section, or who wilfully make a false of falsified report referred to above.

(6) Without prejudice to criminal or civil liabilities for offences connected to money laundering, a financial institution and its employees or a person carrying on a scheduled business that fail to comply with the requirements of this section are liable on conviction to a fine of fifty thousand dollars, and in addition the license of the financial institution to operate as such may be suspended or revoked by the competent authority.

(7) The question whether a reasonable suspicion, for the purpose of subsection (2), has been formed shall be determined objectively having regard to all facts and surrounding circumstances.

"Politically Exposed Person" means any individual who is or has been entrusted with prominent public functions in a foreign country, including a Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials, including family members or close associates of the politically exposed person.

Designated Non-financial Business and Professional means:

1. Casinos including Internet casinos.

2. Trust or company service providers (registered agents) who provide any of the following services to third parties:

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

3. Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for their client concerning the following activities:

a. buying and selling of real estate;
b. managing of client money, securities or other assets;
c. management of bank, savings or securities accounts;
d. organisation 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. Dealing in real estate when the persons dealing are involved in transactions for their client concerning the buying and selling of real estate.

5. Dealing in precious metals, stones - when the persons dealing engage in any cash transaction with a customer.

APPENDIX 2

FORM FOR REPORTING SUSPICION OF MONEY LAUNDERING & TERRORISM FINANCING

To be completed in Triplicate within 5 days of transaction/encounter
CONFIDENTIAL COVER

MINISTRY OF JUSTICE, IMMIGRATION & NATIONAL SECURITY

FINANCIAL INTELLIGENCE UNIT

(IMPORTANT: To be completed within five (5) days of transaction encounter.)

CONFIDENTIAL

FORM FOR REPORTING SUSPICION OF MONEY LAUNDERING

IMPORTANT: Where applicable, all fields must be completed.

MAIL TO:

Director
Financial Intelligence Unit
47 Field's Lane ***(Corner of Field's Lane and Independence Street)***
Roseau
Commonwealth of Dominica

Telephone: (767)-266-3349/74/48/3084/4145/46
Fax: (767)-440-0373
Email: fiu@dominica.gov.dm
Website: www.fiu.gov.dm

NB: Enable "Show/Hide" feature " ¶ " of Microsoft Office Word to read placeholder text.

PART I	STR REPORT DETAILS	
Reporting Entity STR Reference No.:	*THIS FIELD SHOULD NOT BE BLANK.*	
Date:		Date of Original Report:
Code of Reporting Institution: *Choose your Code*		Code of Reporting Officer:
Disclosure Reason:	Terrorism Act 2003 ☐	Money Laundering Act 2011 ☐

PART II	MAIN SUBJECT DETAILS	
(If available, please insert a photo of the subject for identification purposes.)		
	a. INDIVIDUAL	
Click to Select Photo.	Last Name:	Middle Name:
	First Name:	*(Where possible, should not be left blank)* Date of Birth:
	Place of Birth:	Gender:
	Nationality:	Profession:
	Alias:	Nickname:

1. Address				
Street:		City/Community:		
Country:		P.O. Box:		
Telephone (Home)	Telephone (Work)	Telephone (Cell 1)	Telephone (Cell 2)	Fax

CONFIDENTIAL DomFIU STR Form/TF2011

CONFIDENTIAL

2. Address				
Street:		City/Community:		
Country:		P.O. Box:		
Telephone (Home)	Telephone (Work)	Telephone (Cell 1)	Telephone (Cell 2)	Fax
b. COMPANIES				
Name of Company:		Company No.:		
Date of Incorporation: Country of Incorporation:		Company Type: ☐IBC ☐Local Company ☐Trust ☐ Other:		
Registered Office Agent:				
1. Company Address				
Street:		City/Community:		
Country:		P.O. Box:Post Office Box		
Telephone (Home)	Telephone (Work)	Telephone (Cell 1)	Telephone (Cell 2)	Fax
2. Company Address				
Street:		City/Community:		
Country:		P.O. Box:		
Telephone (Home)	Telephone (Work)	Telephone (Cell 1)	Telephone (Cell 2)	Fax
1. Director (s)/Nominee (s)/Beneficial Owners & Address (es)				
Last Name:	First Name:	Middle Name:		
Street:		City/Community:		
Country:		P.O. Box:		
Telephone (Home)	Telephone (Work)	Telephone (Cell 1)	Telephone (Cell 2)	Fax
2. Director (s)/Nominee (s)/Beneficial Owners & Address (es)				
Last Name:	First Name:	Middle Name:		
Street:		City/Community:		
Country:		P.O. Box:		
Telephone (Home)	Telephone (Work)	Telephone (Cell 1)	Telephone (Cell 2)	Fax

PART III	**DETAILS OF IDENTIFICATION (ID) HELD**
a. ID No. 1	
ID Type:	ID Number:
Date of Issue:	Date of Expiry:
ID Remarks:	
Place of Issue:	
b. ID No. 2	
ID Type:	ID Number:

CONFIDENTIAL

Date of Issue:	Date of Expiry:
Place of Issue:	
ID Remarks:	

PART III	MAIN SUBJECT ACCOUNT DETAILS
1. Name of Account:	
Account/Policy Number (s): Account Type: Policy Type:	Date Opened: Date Closed:
Account Currency: ☐Euro (€) ☐US (US) ☐EC (XCD) ☐Pound (£) ☐ Other (Specify):	Name of other bank (s) or financial institution (s) involved in transaction:

a. Authorised Signatory (ies) & Address (es)

Last Name:	First Name:	Middle Name:		
Street:		City/Community:		
Country:		P.O. Box:		
Telephone (Home)	Telephone (Work)	Telephone (Cell 1)	Telephone (Cell 2)	Fax

b. Authorised Signatory (ies) & Address (es)

Last Name:	First Name:	Middle Name:		
Street:		City/Community:		
Country:		P.O. Box:		
Telephone (Home)	Telephone (Work)	Telephone (Cell 1)	Telephone (Cell 2)	Fax

2. Name of Account:	
Account/Policy Number (s): Account Type: Policy Type:	Date Opened: Date Closed:
Account Currency: ☐ Euro (€) ☐US (US) ☐EC (XCD) ☐ Pound (£) ☐ Other (Specify):	Name of other bank (s) or financial institution (s) involved in transaction:

a. Authorised Signatory (ies) & Address (es)

Last Name:	First Name:	Middle Name:		
Street:		City/Community:		
Country:		P.O. Box:		
Telephone (Home)	Telephone (Work)	Telephone (Cell 1)	Telephone (Cell 2)	Fax

b. Authorised Signatory (ies) & Address (es)

Last Name:	First Name:	Middle Name:		
Street:		City/Community:		
Country:		P.O. Box:		
Telephone (Home)	Telephone (Work)	Telephone (Cell 1)	Telephone (Cell 2)	Fax

Enter Information here on third account if necessary:

CONFIDENTIAL DomFIU STR Form/2018 v3

CONFIDENTIAL

PART IV	REASON (S) FOR SUSPICION

IMPORTANT: This section of the report is of critical importance and great care should be taken in completing same. The content of this narrative must, to the extent possible, detail the conduct or activity that will assist in the identification of the possible underlying or identified criminal activity or conduct.

Include in your view, what was unusual, irregular or suspicious about the transaction. The appended checklist is provided as a guide:

- ☐ Describe supporting documentation relied on and retain for 7 years.
- ☐ Explain who benefitted financially or otherwise, from the transaction, by how much, and how.
- ☐ Retain any confession, admission, or explanation of the transaction provided by the suspect and indicate to whom and when it was given.
- ☐ Retain any confession, admission, or explanation of the transaction provided by any other person and indicate to whom and when it was given.
- ☐ Retain any evidence of cover-up or evidence of an attempt to deceive institution.
- ☐ Indicate where the possible violation took place (e.g., main office, branch, other).
- ☐ Indicate where the possible when (or date range, within which) the violation took place.
- ☐ Indicate where the possible what type of instrument or mechanism was involved (e.g., check, travellers check, wire transfer, other).
- ☐ Indicate whether the possible violation is an Isolated incident or relates to other transactions.
- ☐ Indicate whether there is any related litigation; if so, specify.
- ☐ Indicate whether any information has been excluded from this report; if so, why?
- ☐ Indicate whether currency and/or monetary Instruments were involved. If so, provide the amount and/or description.
- ☐ Indicate any account number that may be involved or affected.
- ☐ Recommend any further investigation that might assist law enforcement authorities.

Transacted Amount

*The amount transacted, when transacted in a foreign currency, must also be stated in Eastern Caribbean Currency (XCD).

*XCD	$	TTD	$
USD	$	BD$	$
EURO	€	CAD	$
UK	£	YUAN	¥

Characterisation of Report

This section should be used to append attributes about the report being filed that would better assist in determining how the report should be classified.

Credit Card	☐	Bank Drafts	☐
Insurance Policy	☐	Casino	☐
Large Cash Transaction	☐	Correspondent Accounts	☐
Letters of credit	☐	Credit Card	☐
Drug Trafficking	☐	Fraud	☐

CONFIDENTIAL

Check Kitting	☐	Unusual Large Cash Transaction	☐
Structuring	☐	Smurfing	☐
Money Orders	☐	Digital Currency	☐
Mutual Funds	☐	Large Incoming Wire	☐
Bank Notes	☐	Large Outgoing Wire	☐
Shell Company	☐	Stored Value Cards	☐
Smurfing	☐	Check Kitting	☐
Stocks	☐	Money Laundering	☐
Fraud	☐	Theft	☐
419 Scam	☐	Pyramid Scheme	☐
Money Laundering	☐	False Accounting	☐
Suspicious Inter-bank Transfer	☐	Foreign Exchange Transaction ☐ US ☐ € ☐ CAD ☐ BD$ ☐ XCD ☐ £ ☐ ¥ ☐ TTD	☐
Other:			
Transaction completed		☐ *Yes* ☐ *No*	

Other Relevant Information

Use this section to provide any other information that may assist in understanding the report being filed. This may include but is not limited to, suspicious or unusual activities noticed by the front line staff that may have been appended to the internal report to the Compliance Officer; knowledge of the customer outside of the institution or schedule business.

Code of Compliance Officer:	Date:

PART V **FOR OFFICIAL USE ONLY**

Received by (Position):	Signature	Date
	.....	.....

Entered in Database:	☐ Yes	☐ No
Date Entered:	.....	
Feedback Sent:	☐ Yes	☐ No

APPENDIX 3

APPROVED MARKETS AND EXCHANGES

The following are markets and exchanges approved by the (Financial Intelligence Unit). ***Amendments to this list may be made by the*** Financial Intelligence Unit***from time to time.***

American Stock Exchange (AMEX)

Amsterdam Stock Exchange (Amsterdamse Effectenbeurs)

Antwerp Stock Exchange (Effectenbeurs vennootschap van Antwerpen)

Athens Stock Exchange (ASE)

Australian Stock Exchange

Barbados Stock Exchange

Barcelona Stock Exchange (Bolsa de Valores de Barcelona)

Basle Stock Exchange (Basler Börse)

Belgium Futures & Options Exchange (BELFOX)

Berlin Stock Exchange (Berliner Börse)

Bergen Stock Exchange (Bergen Bors)

Bermuda Stock Exchange

Bilbao Stock Exchange (Borsa de Valores de Bilbao)

Bologna Stock Exchange (Borsa Valori de Bologna)

Bordeaux Stock Exchange

Boston Stock Exchange

Bovespa (São Paulo Stock Exchange)

Bremen Stock Exchange (Bremener Wertpapierbörse)

Brussels Stock Exchange (Société de la Bourse des Valeurs Mobilières/Effecten Beursvennootschap van Brussel)

Cayman Islands Stock Exchange

Cincinnati Stock Exchange

Copenhagen Stock Exchange (Kobenhayns Fondsbors)

Dusseldorf Stock Exchange (Rheinisch-Westfälische Börse zu Düsseldorf)

Florence Stock Exchange (Borsa Valori di Firenze)

Frankfurt Stock Exchange (Frankfurter Wertpapierbörse)

Fukuoka Stock Exchange

Geneva Stock Exchange

Genoa Stock Exchange (Borsa Valori de Genova)

Hamburg Stock Exchange (Hanseatische Vertpapier Börse Hamburg)

Helsinki Stock Exchange (Helsingen Arvopaperipörssi Osuuskunta)

Hong Kong Stock Exchange

Irish Stock Exchange

Jamaica Stock Exchange

Johannesburg Stock Exchange

Korea Stock Exchange

Kuala Lumpur Stock Exchange

Lille Stock Exchange

Lisbon Stock Exchange (Borsa de Valores de Lisboa)

London Stock Exchange (LSE)

Luxembourg Stock Exchange (Société de la Bourse de Luxembourg SA)

Lyon Stock Exchange

Madrid Stock Exchange (Bolsa de Valores de Madrid)

Marseille Stock Exchange

Mexican Stock Exchange (Bolsa Mexicana de Valores)

Midwest Stock Exchange

Milan Stock Exchange (Borsa Valores de Milano)

Montreal Stock Exchange

Munich Stock Exchange (Bayerische Börse in München)

Nagoya Stock Exchange

Naples Stock Exchange (Borsa Valori di Napoli)

NASDAQ (The National Association of Securities Dealers Automated Quotations)

New York Stock Exchange

New Zealand Stock Exchange

OECS Stock Exchange

Oporto Stock Exchange (Bolsa de Valores do Porto)

Osaka Stock Exchange

Oslo Stock Exchange (Oslo Bors)

Pacific Stock Exchange

Palermo Stock Exchange (Borsa Valori di Palermo)

Paris Stock Exchange

Philadelphia Stock Exchange

Rio de Janeiro Stock Exchange (BVRJ)

Rome Stock Exchange (Borsa Valori di Roma)

Singapore Stock Exchange

Stockholm Stock Exchange (Stockholm Fondbörs)

Stuttgart Stock Exchange (Baden-Würtembergische Wertpapierbörse zu Stuttgart)

Taiwan Stock Exchange

Tel Aviv Stock Exchange

The Stock Exchange of Thailand

Tokyo Stock Exchange

Toronto Stock Exchange

Trieste Stock Exchange (Borsa Valori di Trieste)

Trinidad Stock Exchange

Trondheim Stock Exchange (Trondheims Bors)

Turin Stock Exchange (Borsa Valori de Torino)

Valencia Stock Exchange (Borsa de Valores de Valencia)

Vancouver Stock Exchange

Venice Stock Exchange (Borsa Valori de Venezia)

Vienna Stock Exchange (Wiener Wertpapierbörse)

Zurich Stock Exchange (Zürcher Börse)

APPENDIX 4

MEMBERS OF THE FINANCIAL ACTION TASK FORCE

Argentina
Australia
Austria
Belgium
Brazil
Canada
China
Denmark
Finland
France
Germany
Greece
Hong Kong
Iceland
Ireland
Italy
Japan
Luxembourg
Mexico
Netherlands
New Zealand
Norway
Portugal
Russian Federation
Singapore
South Africa
Spain
Sweden
Switzerland
Turkey
United Kingdom
United States of America

The European Commission and the Gulf Cooperation Council

APPENDIX 5

MEMBERS OF THE CARIBBEAN FINANCIAL ACTION TASK FORCE (membership is subject to change):

Anguilla
Antigua & Barbuda
Aruba
The Bahamas
Barbados
Belize
Bermuda
Curacao
St. Kitts & Nevis
St. Lucia
Dominica
El Salvador
Grenada
Guatemala
Guyana
Republic of Haiti
Jamaica
Montserrat
The Netherlands Antilles
Nicaragua
Panama
The British Virgin Islands
The Cayman Islands
St. Vincent & The Grenadines
Suriname The Turks & Caicos Islands
Trinidad & Tobago
Venezuela

The Cooperating and Supporting Nations are:

Canada
The Netherlands
United States of America
France
United Kingdom
Spain

APPENDIX 6

BANKS AND CREDIT UNIONS

EXAMPLES OF SUSPICIOUS ACTIVITY

(Please note that these examples may be applicable to both domestic and offshore banks.)

Two Fundamental Principles:

1. **Get to Know Your Customer:** By applying this principle, you will be able to know the specific conditions of each customer, such as professional activity, trade or business line or corporate purpose. At the same time, you will be able to establish sources of funds and expected account activity.

2. **Inconsistency:** This principle usually appears in all suspicious transactions since there is usually an inconsistency between the transaction and the normal, expected activities of the customer.

These two principles complement each other, since one must get to know the customer in order to be in a position to determine whether the operations are inconsistent with normal business or personal activities.

The transactions listed here are not in and of themselves suspicious, since they require, independent of amount, the application of the fundamental principles relating to "***getting to know your customers"*** and ***"inconsistency"***, in order to be classified as suspicious. These transactions are given only as examples, which, **based on the information available and having applied the above-mentioned principles**, should be considered suspicious. These suspicions should be brought to the attention of the appropriate official within the organization for necessary action.

This list of examples is not exhaustive and must be developed over time. Thus, employees may detect different conditions or criteria that in their opinion, classifies the transaction as suspicious and, therefore, it shall be reported.

Money Laundering Through Cash Transactions

1. When cash deposits are not consistent with the business or profession of the customer.

2. Unusually large deposits or withdrawals of cash by an individual or a legal entity, whose apparent business activities are normally carried out using cheques and other monetary instruments.

3. Substantial increases in cash deposits by any person for no apparent reason, especially if such deposits are subsequently transferred within a short space of time to a destination not normally associated with the customer in question.

4. *Smurfing* or structuring**:** Customers depositing cash on different occasions, in such a way that on each occasion the amount involved is not significant, but all together the total of such deposits equals a very large amount. Smurfing involves the use of more than one customer.

5. Customers seeking to change large quantities of small denomination notes for larger ones, or who frequently change large amounts of cash in foreign currency.

6. Customers whose deposits contain damaged or fraudulent/counterfeit notes.

7. Customers transferring large amounts of money to or from abroad, with instructions for payment to be made in cash.

8. Deposits of large amounts of cash using night depository facilities, thus avoiding direct contact with bank personnel.

9. Frequent or large cash exchanges of local currency to foreign currency or vice versa, without any apparent justification from the professional or commercial activity of the customer.

10. Frequent cash deposits, over the counter or via the night depository, or cash withdrawals of large amounts, without any apparent justification in terms of the type and volume of the business in question.

11. Proposals of large operations involving the sale of foreign bank notes (principally US dollars) or cheques drawn in foreign currency against local currency, made by persons claiming to be intermediaries or commission agents. On occasion such persons allege

supposed contacts with the local authorities and even the awareness of the Central Bank with respect to the carrying out of such operations.

12. When deposits are detected from various locations, in large amounts of cash mainly with low denominations notes.

13. When accounts are detected that receives frequent deposits involving large foreign currency amounts.

Money Laundering Through Bank Accounts and Other Facilities

1. Customers not acting on their own behalf and who refuse to reveal the true identity of the beneficiary.

2. When insufficient, false, or suspicious information is provided by the customer or prospective customer, or providing information which is difficult or expensive to verify.

3. Customers refusing to provide information, which under normal circumstances would permit access to credit facilities or other, valuable banking services.

4. Customers holding several accounts and making deposits in cash in each of them, in such a way that the total amount deposited is considerable. This is another example of "structuring" deposits.

5. Any persons whose accounts show virtually no banking activity, but are used to receive or pay significant amounts not clearly related to the account holder and/or his business (e.g. a substantial increase in the volume of an account.)

6. The withdrawal of large amounts from an account previously dormant or inactive, or from an account, which has just been credited with a large amount unexpectedly from abroad.

7. Customers maintaining accounts with several financial institutions in the same city or town, especially when the bank is aware of the existence of a regular consolidation process of such accounts prior to a request for a transfer of the funds.

8. The balancing of payments (debits) with deposits (credits) made in cash the same day or the previous day.

9. Frequent deposits and withdrawals to and from accounts consistently in rounded numbers, e.g. $20,000, $40,000, $55,000, $100,000 that is inconsistent with known business activity of the customer. Please note that more sophisticated launderers may not use rounded numbers in order to simulate ordinary business payments.

10. Customers who together and simultaneously use separate cashiers to carry out substantial operations in cash or foreign currency.

11. Increased use of safety deposit boxes. Increased activity by the persons concerned. The depositing and withdrawal of sealed packages.

12. Company representatives avoiding contact with the office.

13. Frequent and/or substantial increases in cash deposits or deposits of negotiable instruments by a professional firm or company (e.g. a trust or nominee company) using accounts opened in the name of the client of such company, especially if such deposits are quickly transferred to another client account.

14. Insufficient use of the normal advantages offered by banks, such as avoiding high interest rates for important balances.

15. Whenever a large number of individuals deposit cash in the same account without an appropriate explanation.

16. When the purchase and/or deposits of monetary instruments are not consistent with the business or profession of the customer.

17. Wire transfer activity, which is not consistent with the business or profession of the customer.

18. When customers are detected that receives funds transfers and immediately transforms them into monetary instruments in the name of third parties.

19. A large volume of deposits to one or several different accounts with frequent transfer of a major portion of the balances to an account(s) at the same or other bank.

20. When accounts are detected involving a large number of deposits in cashiers' cheques, money orders and/or wire transfers.

21. When accounts are detected where several deposits are made in different branches on the same day.

22. When accounts are detected that receive in one day or during a short period, several small deposits through transfers, cheques and money orders, which immediately transfer such funds to another location, town, city or country e.g. through wire transfers, leaving only a small amount as a balance in the account.

23. When accounts are detected that receive and send wire transfers very often, especially with countries considered high-risk money laundering jurisdictions (e.g. major drug

producing/consuming/transit countries), or those with strict banking secrecy laws. Pay special attention if operations of this type are made through banks, which are small private, or, "shell" banks or banks of which little is known.

24. When the domicile of a customer's account does not correspond with the service area of the branch in which the customer normally transacts.

25. Large and/or frequent deposits by customers who claim that the funds are lottery or casino winnings.

Money Laundering Through Loans With or Without Collateral

1. Loans without a clear purpose.

2. Customers unexpectedly paying off problem loans, without justification of the fund's origin.

3. Loans completely or partially paid off from unknown sources in cash, foreign currency or by instruments not identifying their issuer.

4. Loans that are repaid with funds deposited in another institution by third parties, the origin of which is unknown or the value of which bears no relation with the customer's situation.

5. A request for a loan backed by assets deposited in the financial entity (e.g. deposits) or by third parties, the source of which is unknown or the value of which has no relation to the situation of the customer.

6. A request for financing, when the source of the financial contribution of the customer with respect to a business is unclear, particularly if it refers to real estate.

7. Loans guaranteed by third parties with apparently no relation to the customer.

8. Loans secured by property in which the disbursement will be made in another jurisdiction.

9. Requests for credit facilities from little known customers who offer guarantees in cash, financial assets, foreign currency deposits or foreign bank guarantees, and whose business bears no relation to the object of the operation.

10. When a guarantee for the disbursement of credit operations is left to be enforced, the amount having been used for legal trading activities or transferred to another company, person or entity, without any apparent justification.

11. When there are letters of credit documenting imports and exports about which there is no information regarding the importer or exporter, in accordance with established standards.

12. When standby letters of credit are detected guaranteeing loans granted by foreign financial entities, without any apparent economic justification.

Money Laundering Involving the use of Credit Union Accounts

1. Credit Unions must apply all of the above provisions with regard to cash, banks, loans and offshore activities

2. Credit Unions should pay particular attention to the 10 highest depositors and the 10 highest creditors and be aware of the risk to the Union of failure of any one or more of them.

3. Credit Unions should be aware of the local Politically Exposed Person (PEP) who might influence the staff or the board to treat certain transactions in a different way or to turn a blind eye to certain activities because it appears to be in the best interest of the Union.

4. Credit Union staff should be aware of members circumstances and raise questions about deposits of cash from a member who is knowingly unemployed or where for instance unusual deposits are made which although within reporting limits are out of character with the expectation.

Money Laundering Through (Other) Offshore Activities

1. Customers who frequently have operations with companies or financial institutions located in countries with strict secrecy laws and without effective supervisory or regulatory structures.

2. A customer introduced by a foreign branch, affiliate or bank based in a country where drug production or trafficking is frequent.

3. The use of Letters of Credit and other offshore mechanisms for moving money between countries where such activity bears no relation to the customer's normal business.

4. Use of back-to-back loans where deposits securing the loans are with offshore entities and the loans are granted and disbursed to other parties in another jurisdiction.

5. Use by customers of cash secured international credit cards (or debit cards) issued by offshore entities and frequent use of ATM or other banking facilities to withdraw cash.

6. The creation of large balances in accounts, which are not consistent with the customer's business, and subsequent transfers to accounts offshore.

7. Electronic funds transfers, without any explanation by customers, involving an immediate deposit and withdrawal from the account or even without passing through an account (e.g. use of omnibus, suspense or consolidation accounts).

8. Use of **Payable Through Accounts** where the beneficiaries of the accounts are unknown or where they are clients of offshore entities with strict secrecy laws.

9. Frequent requests for travellers' cheques, foreign denomination drafts or other negotiable instruments without a clear purpose.

10. Frequent deposits in an account of travellers' cheques or foreign denomination drafts, especially if originating from abroad without a clear purpose.

11. Frequent deposits to customer accounts originating from "casa de cambios" located in countries with inadequate regulations, especially where the customer is a broker or acting as an intermediary for others.

12. Customers who deposit loan proceeds borrowed from offshore institutions where the source of the funds is unknown, especially if conducted through offshore corporations, trust or nominee arrangements.

13. Cash deposits from offshore correspondent banks where the frequency and volume of deposits are substantial in view of the size, nature and location of the client bank

APPENDIX 7

INVESTMENTS RELATED TRANSACTIONS

EXAMPLES OF SUSPICIOUS ACTIVITY

(Please note that these examples may be applicable to both domestic and offshore banks.)

Money Laundering Through Investments Related Transactions

1. The purchase of securities to be kept in custody by the financial institution where such operation appears to be inconsistent with the customer's business.

2. Requests from customers for investment handling services, in foreign currency or securities, where the source of the funds is not clear or is inconsistent with the customer's known business.

3. The purchase by customers of bearer shares, especially if issued by offshore entities, and where custody or control of such shares is unknown.

4. The purchase and sale of financial instruments without any apparent purpose or in unusual circumstances.

5. Securities transactions through a trust or similar intermediary where the amounts are substantial and are in cash, or are made through an offshore entity bearing no relation to the customer's business.

APPENDIX 8

INSURANCE COMPANIES AND INSURANCE PRODUCTS EXAMPLES OF SUSPICIOUS ACTIVITY

1. Insurance companies rarely expect to be the target of money launderers because of the long term nature of the contracts and significant penalties on repayment.

2. Single Premium policies can be used in the layering of laundered money by providing the client with a company cheque on cancellation at the end of a cooling off period.

3. Similar arrangements can apply to other packaged and wrapped products and indeed annuities.

4. Insurance companies should decline to accept cash payments and should always remit funds back directly to the account from which they were originally transmitted.

APPENDIX 9

DESIGNATED NON-FINANCIAL BUSINESSES & PROFESSIONS EXAMPLES OF SUSPICIOUS ACTIVITY

Money Laundering Involving Real Estate Agents and Property

1. Real Estate agents are now at the fore of money laundering prevention and should always fully know their client and properly establish the source of the clients funds.

2. The purchase of land and property is a desirable use of funds for money launderers as values over time tend to rise especially if they can become involved in property development.

3. A classic model commences with the purchase of a parcel of land with development potential for hotels and or timeshares.

4. Cash is the preferred format when used to seek advantage in planning applications and with corrupt officials.

5. Builders traditionally are paid in cash which is ideally suited to money laundering activity.

6. Timeshares provide cash flow but also explanation for lack of occupancy.

7. Ancillary services such as car hire, pizza delivery and shops and watersports all generate activity to support depositing of cash with banks.

8. Hotels with casinos provide the pinnacle of opportunity for money laundering activity.

Money Laundering Through Trusts

1. When a trust owning real or other property is detected and a foreign individual or legal entity not fully identified to the bank is named as beneficiary.

2. When property is contributed to a trust without identifying the settlor or the source of funds.

3. Trusts without clear purposes.

4. When trust property constitutes companies registered in offshore jurisdictions, especially where shares are in bearer form, where custody or control of the shares is unknown, or where the source and amount of company assets are unknown.

5. When the trust document (e.g. declaration or deed) does not convey substantive control of trust property to the trustee and where control rests with other parties, e.g. settlor or beneficiaries or where the settlor is appointed manager of assets held in trust.

Money Laundering Involving the High Value Items (Dealers in precious Metals and Jewels and Motor Cars and Boats)

1. Jewellery is traditionally favoured by money launderers because items of very high value can be hidden, moved easily and yet discretely across borders by a large number of people yet paid for in cash.

2. Precious stones have a value which is assessed by a common worldwide standard that is not subject to great fluctuations when say compared with interest rates. The fact that the value is effectively inflation proof yet can be transferred by delivery is a very powerful benefit.

3. Jewellers need to pay attention to not only those whom they supply but also those who supply them. Cash transactions should be discouraged and it should be remembered that the reporting requirement already applies to transactions above agreed limits.

4. Dealers in other high value items must remain vigilant to their being used to assist in money laundering. For example someone who changes his car or boat rapidly at a loss for each transaction should be treated with some suspicion.

5. Cars and boats now change hands at increasingly significant figures and by their very nature have the capacity to move from one place to the next. Luxury cars like Ferraris and Aston Martins are transported around the world yet still retain their premium value irrespective of currency.

Money Laundering Involving the use of E-Gaming Businesses

1. E-Gaming businesses generally believe that they are protected from money laundering because they do not accept cash from punters which in its simplistic form is correct.

2. This does not however preclude layering if the gaming house will accept instructions to remit funds to third parties or different accounts to that which the money was originally provided from.

3. Jurisdictions authorising or overseeing e-gaming businesses must be extra vigilant to prevent money launderers setting up their own casinos/sites which they could then use to distribute the proceeds of crime to third parties.

4. E-gaming providers setting up poker services take a turn on all games and players monies go from one to another. This system could become an advanced payments vehicle for money launderers if they were able to influence who was sat at the table of a particular provider.

5. Providers should complete detailed due diligence before sending winning clients payments in excess of reporting limits (EC$ 10,000)

APPENDIX 10

EMPLOYEES & OFFICIALS OF FINANCIAL INSTITUIONS EXAMPLES OF SUSPICIOUS ACTIVITY

1. Unexplained changes in the employee's behaviour and lifestyle e.g. lavish lifestyle, avoidance of holidays, association with known drug traffickers, criminals, etc.

2. Significant and abnormal changes in performance by the employee such as when an unexpected large increase in the sale of cash products is observed.

3. Any dealings with an employee where the identity of the final beneficiary of the institution's services or products is unknown or concealed, contrary to normal operating procedures on identification and source of funds.

4. Employees acting as agents for customers to effect transactions on customers' accounts, safety deposit boxes, etc.

APPENDIX 11

ACCOUNTS UNDER INVESTIGATION OR LEGAL PROCEEDINGS

1. Whenever an account or customer is the subject of investigations, service of legal process, accusation, seizure or restraining order, or other action relating to money laundering, fraud or other illegal activity in the country or abroad.

2. Any account which is the source or receiver of a significant amount of funds related to an account or customer who the subject of legal proceedings by a Court or authority in connection money laundering, fraud or other illegal activity in the country or abroad.

3. Any account controlled by the signatory of another account, which is under investigation, or the subject of legal proceedings by a Court or authority in connection with fraud or money laundering in the country or abroad.

4. Any account or customer who is the subject of warning circulars or similar notices from regulatory or other sources in relation to illegal or improper business conduct.

APPENDIX 12

INFORMATION SOURCES

Useful Contacts:

The following list provides the web-sites for many international bodies who can provide useful additional material with regard to financial regulation and anti-money laundering.

1. **www.imf.org**
2. **www.oecd.org**
3. **www.fatf-gafi.org**
4. **www.cfatf.org**
5. **www.bis.org/fsi**
6. **www.iosco.org**
7. **www.iaisweb.org**
8. **www.wolfsbergprinciples.com**
9. **www.ogbs.net**
10. **www.egmontgroup.org**
11. **www.transparencyinternational.org**

APPENDIX 13

CERTIFICATION OF IDENTIFICATION DOCUMENTS

A certifier must be a suitable person, such as a lawyer, accountant, director or manager of a regulated institution, a notary public, a member of the judiciary, a senior civil servant, a consular official or a serving police officer.

The certifier should sign and date the copy document (printing his name clearly in capitals below), state that it is a true copy of the original, and clearly indicate his position or capacity on it. If a covering letter is used it is important to establish the document to which the letter refers.

Where certified documents are accepted it is up to the FSP to satisfy himself that the certifier is appropriate.