

**KNOW YOUR CUSTOMER  
GUIDELINES**

**FOR**

**LICENSED FINANCIAL  
INSTITUTIONS**

**Central Bank of Barbados  
March 2001**

## TABLE OF CONTENTS

	<b>Foreword</b>	<b>1</b>
<b>1</b>	<b>Introduction</b>	<b>3</b>
	Purpose of Guidelines	
	International Background	
	Definition of Money Laundering	
<b>2</b>	<b>Legislation and Regulatory Framework</b>	<b>7</b>
	Legislation	
	Offences	
	Scope of Guidelines	
<b>3</b>	<b>Identification Procedures</b>	<b>11</b>
	Direct Applications: Personal Client	
	Direct Applications: Body Corporate	
	Indirect Applications	
	Exemptions	
	Trust, Nominee and Fiduciary Customers	
<b>4</b>	<b>Internal Controls and Procedures</b>	<b>16</b>
<b>5</b>	<b>Record Keeping</b>	<b>18</b>
<b>6</b>	<b>Reporting</b>	<b>20</b>
<b>7</b>	<b>Training and Awareness</b>	<b>23</b>
	<b>Appendices</b>	<b>26</b>
	- FATF Member Countries and Observer Bodies/Organizations	
	- The Forty Recommendations	
	- CFATF Member Countries; Cooperating/Supporting Nations; Observers	
	- The Nineteen Recommendations	
	- Basle Statement of Principles	
	- Customer Reference Request Form	
	- Identification Exemption	
	- Large Transaction Report	
	- Examples of Suspicious Transactions	
	- Suspect Transaction Report	

## CENTRAL BANK OF BARBADOS

### **KNOW YOUR CUSTOMER GUIDELINES FOR LICENSED FINANCIAL INSTITUTIONS** Issued in conjunction with the Anti-Money Laundering Authority pursuant to its powers under the Money Laundering (Prevention & Control) Act.

#### **FOREWORD**

The Central Bank of Barbados first issued guidelines on this subject to financial institutions licensed under the Offshore Banking Act and the Financial Intermediaries Regulatory Act (now Financial Institutions Act) in April 1991 following the issuance of the Forty Recommendations by the Financial Action Task Force<sup>1</sup> (FATF) a year earlier. In association with regional Central Banks, the Central Bank of Barbados revised and reissued new guidelines in March 1995. These notes provided guidance to financial institutions on the requirements for effective systems and controls in the fight against money laundering.

Barbados has actively participated in the work of the Caribbean Financial Action Task Force<sup>2</sup> (CFATF), the regional chapter of the FATF. The Government of Barbados has enacted comprehensive legislation to address the issue of money laundering. More recently, the Money Laundering (Prevention And Control) Act, 1998-38 ("the Act") was proclaimed and an Anti-Money Laundering Authority<sup>3</sup> ("the Authority") and Financial Intelligence Unit were established. In light of the enactment of new legislation in April 2000 and ongoing international developments to improve regulatory standards, the Central Bank of Barbados is now revising its anti-money laundering guidelines.

Financial institutions should ensure that the guidelines are also applied to their branches and subsidiaries abroad, especially in countries which do not or insufficiently apply similar recommendations, to the extent that local applicable laws and regulations permit. Financial institutions should inform the Central Bank of Barbados ("Central Bank) and the Authority when the local applicable laws and regulations prohibit the

---

1 The FATF develops and promotes policies to combat money laundering. Refer to section 1.02 of the guidelines.

2 The CFATF presents a regional perspective to the money laundering issue. Refer to section 1.02 of the guidelines.

3 The Authority was established in August 2000 and its responsibilities are shown in section 2.0 of the guidelines.

implementation of these guidelines.

The guidelines will be used by the Central Bank in the assessment of the adequacy of anti-money laundering systems in place at licensed financial institutions.

## SECTION 1 INTRODUCTION

### 1.01 Purpose of Guidelines

In order to preserve the viability and reputation of Barbados' financial sector, financial institutions must be vigilant to guard against money laundering. Financial institutions may be attractive to money launderers in light of the variety of their services and instruments that can be used to conceal the source of money. The placement and transfer of cash in the financial system are stages at which money laundering is most easily detected. These guidelines represent good industry practice and compliance will assist institutions in identifying attempts to launder criminal proceeds through the financial system. Financial institutions that have adequate prevention systems in place are best able to recognise and detect efforts to launder money.

One of the most effective methods to combat money laundering is a sound knowledge of a customer's business and pattern of financial transactions and commitments. The adoption of "know-your-customer" rules does not only make good business sense but is an essential tool to avoid legitimising the proceeds of criminal activity. The main concepts of "know-your-customer" are:

- (a) Identification procedures and monitoring;
- (b) Suspicious transaction reporting (allied to adequate record keeping); and
- (c) Controls and communication (allied to training and awareness).

In recent times, the concept of know-your-customer has been extended to ensure that institutions know those with whom they are doing business, including employees, correspondent banks and regulators. The overriding goal remains unchanged, that is, the financial institution's ability to review their customers' activities for unusual activity.

Persons and entities other than financial institutions are also vulnerable to money launderers. To this end,

those engaged in any of the following activities should be aware of the guidelines and are encouraged to use this document to safeguard their operations: -

- (1) Financial service providers and consultants;
- (2) Money exchange houses such as bureaux de change, cheque encashment;
- (3) Money transmission services including wire transfers;
- (4) Bookmaking/gaming services;
- (5) Dealers in motor vehicles, jewellery, art and antiques;
- (6) Professional accountants and other persons engaged in accounting and bookkeeping services;
- (7) Management services including investment management;
- (8) Services relating to company registration and incorporation, the provision of company secretary services and registered offices for companies;
- (9) Trustee services including the provision of trust investment advice; and
- (10) Advice, administration and other services provided in the course of business relating to real estate.

Notwithstanding the definition of a financial institution in section 2 of the Act, entities such as domestic trusts, partnerships, attorneys-at-law, management companies, and post offices should consider the issues embodied in these guidelines. This would serve to protect them from the possibility of committing an offence of money laundering.

## **1.02 International Background**

Regulators worldwide share a common goal in the fight against money laundering. Guidance notes and principles have been issued by several regulatory agencies in an effort to harmonise supervisory standards and more effectively combat criminal activity. The know-your-customer principle is a fundamental requirement for an effective anti-money laundering programme and its importance is emphasised in all regulatory guidelines.

The Financial Action Task Force (FATF) is an inter-governmental body which develops and promotes policies to combat money laundering. The FATF was established by the G-7 Summit in Paris in 1989 and currently has 29 member countries and two regional organisations. The current members are listed at **Appendix 1**. In 1990, the FATF issued 40 Recommendations to be implemented to fight money laundering and these were subsequently revised in 1996. The 40 Recommendations have become the internationally accepted anti-money laundering standard. (See **Appendix 2**).

The Caribbean Financial Action Task Force (CFATF) is an organisation of states and territories of the Caribbean basin which has agreed to implement common counter-measures against money laundering. The CFATF originated in early 1990 and holds observer status with the FATF. Barbados is a member of this body whose membership currently stands at 26. (See **Appendix 3**). In June 1990, the CFATF issued 19 Recommendations to complement the FATF's 40 Recommendations by presenting a regional perspective to the issue. (See **Appendix 4**).

In order to assess the status of the anti-money laundering framework of their member countries, both the FATF and the CFATF undertake detailed reviews referred to as mutual evaluations. A CFATF mutual evaluation of Barbados was completed in September 1997.

In September 1997, the Basle Committee on Banking Supervision issued a paper entitled the "Core Principles For Effective Banking Supervision" which includes a requirement (principle 15) that supervisors "determine that banks have adequate policies, practices and procedures in place, including strict *know-your-customer* rules, that promote high ethical and professional standards in the financial sector and prevent the bank being used, intentionally or unintentionally, by criminal elements." The Committee also issued a Statement of Principles in December 1988 entitled Prevention of Criminal Use Of The Banking System For The Purpose Of Money Laundering. (See **Appendix 5**).

Recently, there has been increased pressure from such bodies as the FATF, the Organisation for Economic

Cooperation and Development (OECD) and the U.S. Treasury for countries to strengthen their anti-money laundering framework. Barbados remains committed to implementing adequate measures to combat money laundering.

### **1.03 Definition of Money Laundering**

Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of criminal activities. If undertaken successfully, the money can lose its criminal identity and appear to be legitimately derived.

In simple terms, the money launderer's goal is to: -

- (1) Place the money in the financial system, without arousing suspicion;
- (2) Move the money around, within or across multiple jurisdictions, and often in a series of complex transactions, so that it becomes difficult to identify its original source;
- (3) Then move the money back into the financial and business system, so that it appears as legitimate funds or assets.

There is no one method of laundering money. Initially, however in the case of drug trafficking and other serious crimes, the proceeds usually take the form of cash which needs to enter the financial system by some means. The laundering process involves three sometimes overlapping stages: -

- (1) Placement: Physically disposing cash proceeds derived from illegal activities;
- (2) Layering: Separating the proceeds from criminal activity from their origins through layers of complex financial transactions;
- (3) Integration: Providing an apparent legitimate explanation for the illicit proceeds.

The three basic steps occur as separate and distinct stages but may occur simultaneously or, more commonly, they may overlap. The available laundering mechanisms and requirements of the criminal organization shape how these stages are employed.

## SECTION 2 LEGISLATIVE AND REGULATORY FRAMEWORK

### 2.01 Legislation

Between 1990 and 2000, the Government of Barbados enacted several pieces of legislation aimed at preventing and detecting drug trafficking, money laundering and other serious crimes. These are the: -

- (a) Drug Abuse (Prevention and Control) Act, 1990;
- (b) Proceeds of Crime Act, 1990-13;
- (c) Mutual Assistance in Criminal Matters Act, 1992; and
- (d) Money Laundering (Prevention and Control) Act, 1998-38. ("the Act")

The Money Laundering (Prevention and Control) Act, 1998-38 confers responsibility for the supervision of financial institutions to the Anti-Money Laundering Authority ("the Authority") which was officially established in August 2000. A Financial Intelligence Unit has been established to carry out the Authority's Anti-Money Laundering supervisory function over financial institutions including the functions of collecting, analyzing and disseminating suspect transaction reports. Where the Authority believes on reasonable grounds that a transaction involves proceeds of crime the Authority sends the report to the Commissioner of Police. A Financial Investigations Unit has been established within the Royal Barbados Police Force to investigate reports referred to it by the Authority.

The Act establishes a mandatory threshold of BDS\$10,000 (or its equivalent in foreign currency) for the retention of business transaction records. This requirement will facilitate a system to help identify money launderers.

This framework is supported by the Central Bank of Barbados which is responsible for financial institutions licensed under the Financial Institutions Act, 1996 and the Offshore Banking Act, 1979. The Bank Supervision

Department has included know-your-customer verification within the scope of onsite examinations since 1997.

## 2.02 Offences

Section 3(1) of the Money Laundering (Prevention and Control) Act states that a person engages in money laundering where:

- (1) The person engages, directly or indirectly, in a transaction that involves money or other property, that is proceeds of crime; or
- (2) The person receives, possesses, conceals, disposes of, or brings into or sends out of Barbados, any money or other property that is proceeds of crime.

It is not necessary for the original offence from which the proceeds stem to be committed in Barbados, so long as it would have been an offence had it taken place within Barbados. See sub-section 3(4).

The offences and their associated penalties appear in Sections 12, 20, 21 and 22 of the Act and are summarized as follows:

- A person who has been convicted of an indictable offence is not permitted to be licensed to carry on the business of a financial institution; and where the person is a financial institution the licence will be revoked. See Section 12(1).
- Engaging in the act of money laundering is punishable on conviction to a maximum of 25 years imprisonment, a fine of \$2.0 million or both. See Sub-section 20(3).
- Aiding, abetting, counseling or conspiring to engage in a transaction involving money or property

that is or is suspected to be the proceeds of crime is punishable on conviction to a maximum of 15 years imprisonment, a fine of \$1.5 million or both. See Sub-section 20(4).

- Where an offence is committed under Section 20 by a body of persons, whether corporate or unincorporated, every person acting in an official capacity for or on behalf of such a body at the time of the commission of the offence, is guilty of that offence and will be tried and punished accordingly. See Section 21.
- (a) Tipping off the target or third party about an investigation or pending investigation into money laundering or freezing order; disposing, destroying or falsifying material evidence all of which may result in the investigation being prejudiced. See Sub-section 22(1); or
  - (b) Falsifying, concealing, destroying or otherwise disposing of, or causing or permitting the falsification, concealment, destruction or disposal of any document or thing that is likely to be material to the execution of a freezing order. See Sub-section 22(2); or
  - (c) Disclosing the existence of a freezing order (on the property of, or in the possession or under the control of a person suspected of money laundering) to an unauthorised person as defined in the Act. See Sub-section 22(3);
  - (d) Is punishable on conviction to a maximum of 2 years imprisonment a fine of \$50,000 or both.

### **2.03 Scope of Guidelines**

Although the Money Laundering (Prevention And Control) Act applies to all persons and businesses, additional administrative requirements are placed on financial institutions which are defined as:

- (1) Any persons carrying on business under the Financial Institutions Act; and
- (2) Includes

- A deposit taking institution
- A credit union within the meaning of the Co-operatives Societies Act
- A building within the Building Societies Act
- A friendly society within the meaning of the Friendly Societies Act
- An insurance business within the meaning of the Insurance Act
- An offshore bank within the meaning of the Offshore Banking Act
- An exempt insurance company within the meaning of the Exempt Insurance Act
- An international business company within the meaning of the International Business Companies Act
- A society with restricted liability within the meaning of the Societies with Restricted Liability Act, 1995
- A foreign sales corporation within the meaning of the Barbados Foreign Sales Corporation Act
- A mutual fund, mutual funds administrator and a mutual fund manager
- International trusts within the meaning of the International trusts Act, 1995.

### **SECTION 3 IDENTIFICATION PROCEDURES**

Financial institutions are required to document and implement effective procedures to prevent money laundering. Employees should be aware of these procedures and apply them in order to verify and adequately document the identity of the customer or account holder.

Financial institutions should reassess their requirements pertaining to identification records to ensure that all customer records conform to the new requirements. In addition, customer identification records should be verified periodically to ensure that identification information remains current. Any change in the name and address of any customer from that given when the business relationship was first established should be recorded.

A customer or account holder refers to any nominee, agent, beneficiary or principal engaged in a business transaction as defined in Section 2 of the Act.

Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names. It is a requirement to identify, on the basis of an official or other reliable identifying document, and record the identity of clients, either occasional or usual, when establishing business relations or conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe-deposit boxes, the use of safe custody facilities, performing of business transactions in excess of the \$10,000 threshold).

Financial institutions should exercise extreme caution in their business relations and transactions with persons, including companies and financial institutions from other countries. Where possible, contact should be made with appropriate persons in these countries as part of know-your-customer procedures.

At a minimum, there should be adherence to the following guidelines: -

### 3.01 Direct Applications: Personal Client

1. Institutions are required to obtain relevant identification records of a customer as indicated in Section 2 of the Act. The following information should be ascertained:

- (1) Full name(s) and aliases;
- (2) Permanent address\*;
- (3) Date and place of birth;
- (4) Nationality;
- (5) Reason for opening the account;
- (6) Nature and place of business/occupation;
- (7) Expected account turnover and source of funds; and
- (8) Any other information deemed appropriate by the institution.

2. At a minimum, valid photo-bearing identification should be obtained, e.g.

- (1) Passport; or
- (2) National identification card; or
- (3) Drivers licence; and  
Where the applicant is non-resident,
- (4) Social security number

In instances where original documents are not available, copies should only be acceptable if certified by a notary public (e.g. justice of the peace). Identification documents which do not bear a photograph or signature and which are easily obtainable (e.g. birth certificate) should not be accepted as the sole means of

identification. The financial institution is ultimately responsible for verifying the name and address of the applicant.

\* Any address referred to in the guidelines relates to a permanent address. Temporary addresses, post office boxes and in-care-of addresses are not acceptable under know-your-customer rules.

The Act does not recognise introduction or referrals in whole or in part, as an alternative to proper identification procedures. The onus remains on the institution to separately verify the identity of the customer.

Where references are used as one of the means of verification, the information should be documented to form part of the identification record. See specimen format at **Appendix 6**. An account holder's identity should not be established solely on the basis of a referral.

References should be considered from:

- A financial institution as defined in Section 2(1) of the Act; or
- A reputable financial institution which the bank has satisfied itself by way of reasonable measures.

Financial institutions undertaking business transactions with persons from these approved countries are required to exercise the appropriate due diligence that is consistent with good banking practice.

### **3.02 Direct Applications: Body Corporate**

The relevant requirements in 3.01 are also applicable to a body corporate. Financial institutions should verify the identity of the directors, shareholders, officers, account signatories and beneficial owners. In the latter instance, an affidavit should be obtained confirming the beneficial ownership.

In addition to the requirements for a certificate of incorporation, certificate of continuance and certificate of registration (see Section 2 of the Act), certified copies of the following should also be obtained at a minimum:

- (1) Partnership agreement;
- (2) Memorandum and articles of association;
- (3) Certificate of good standing; and
- (4) By-laws;

### **3.03 Indirect Applications**

All prospective applicants are subject to the same proof of identification and verification as outlined in 3.01 and 3.02 regardless of the manner in which the application is submitted to a financial institution.

An account should not be opened by any means other than by establishing in person the identity of a customer through the account holder's own identity documents. Where due diligence on a prospective customer has been completed by a branch or banking subsidiary/affiliate of the financial institution and that process meets the criteria of the Barbados guidelines, then copies of the relevant documentation must be obtained before the account is opened. In the case of an international bank engaged in intra group treasury operations, written confirmation of the source of funds must be obtained from the parent company.

### **3.04 Exceptions to Identification Requirements**

Section 7(5) of the Act permits the exception of the production of any evidence of identification only where the applicant is itself a financial institution subject to Part II of the Act or where a series of transactions occur in a business relationship for which the applicant has already produced satisfactory evidence of identity. A definition of a financial institution appears in sub-section 2(1) of the Act is reproduced in Section 2.03 of the guidelines.

The institution is expected to document those instances where this section of the Act is applied. See

**Appendix 7** for a specimen format.

### **3.05 Trust, nominee and fiduciary customers**

Financial institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction is conducted if there are any doubts as to whether these clients or customers are not acting on their own behalf, in particular, in the case of domiciliary companies (i.e. institutions, corporations, foundations, trusts, etc. that do not conduct any commercial or manufacturing business or any form of commercial operation in the country where their registered office is located).

At a minimum, the financial institutions should obtain and verify the following information: -

- (1) Evidence of the appointment of trustees (e.g. extracts from Deed of Trust);
- (2) Nature and purpose of the trust;
- (3) Verification of the identity of the trustee, settlor, protector; person providing the funds; controller or similar person holding power to appoint or remove the trustee; and
- (4) Source of funds.

## SECTION 4 INTERNAL CONTROLS AND PROCEDURES

Financial institutions should develop and document an anti-money laundering program to ensure compliance with the Act. It is required that institutions:

- (i) Develop and apply internal policies, procedures and controls to combat money laundering. Sub-section 8(1)(e)(i).
- (ii) Develop audit functions to evaluate such policies, procedures and controls. Sub-section 8(1)(e)(ii); and
- (iii) Develop a procedure to audit compliance with section 8 of the Act. Sub-section 8(1)(g).

Programs should be implemented which are applicable for the size and nature of the institution's operations and include, as a minimum:

- (a) Adequate internal policies, procedures and controls which include -
  - Opening of accounts and documentation requirements;
  - Designating a local compliance officer(s) at the management level to coordinate and monitor the compliance program, receive internal reports and issue external reports to the Authority (see Section 9 of the Act);
  - Establishing management information/reporting systems to facilitate the timely detection and reporting of suspicious activity within the institution and to the Authority;
  - Screening procedures to ensure high standards not only when hiring employees but on an ongoing basis.
- (b) An ongoing employee training program (see Section 10 of the Act). Refer to section 7 of the guidelines.

- (c) An effective risk-based audit function to test and evaluate the compliance program. This should include assessments of compliance with internal reporting, record keeping and reporting to the Authority. See sub-section 8(1)(e) and (g).

Section 8 of the Act establishes a threshold level of BDS\$10,000 or its equivalent in foreign currency for document retention. Financial institutions are expected to be vigilant in their monitoring to ensure that linked transactions, which are individually below the BDS\$10,000 limit but with an aggregate value exceeding the threshold are monitored and appropriately recorded.

#### **4.01 Complex Transactions/Wire Transfers**

All institutions should review and properly document the background and purpose of all complex, unusual, large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

Institutions should exercise caution in accepting funds from non-account holders and non-correspondent banks for wire transfers to unknown third parties. The name and address of the ordering and beneficiary customers should be included on all domestic and international transfers. Each institution that participates in a business transaction via wire transfer should relay this "identifying" information about the transfer to any other financial institution participating in the transmittal.

Procedures should be identified to detect suspicious activity in all types of business transactions undertaken by the institution including cash, wire transfers, cheques, credit and debit cards, automatic teller machine transactions and on-line banking.

## SECTION 5 RECORD KEEPING

Financial institutions should maintain for a minimum of five years, all business transaction records (both domestic and international) of all transactions exceeding \$10,000 to enable them to comply swiftly with information requests from the Authority. It may be necessary for institutions to retain business transaction records for a period exceeding the date of termination of the last business transaction where certain circumstances predate this event, for example:

- (a) Date of closure of an account;
- (b) Date of termination of the business relationship; or
- (c) Date of insolvency.

Where there has been a report of a suspicious transaction or there is an on-going investigation relating to a transaction or client, the institution should retain the documentation until such time as advised by the Authority or High Court.

Financial institutions should ensure that their document retention policy conforms with the stipulations of the Act.

Business transaction records must be kept in sufficient form to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour. See Sections 8(1)(a) and (3) of the Act. These documents should be available to domestic law enforcement authorities in the context of relevant criminal prosecutions and investigations.

Documentation refers *inter alia* to any part of a document, reproduction, copies, microfiche, computerised or electronic form. See sub-section 2(2).

Institutions should retain customer identification records, account files and business correspondence since it may be necessary to establish a financial profile of any suspected account as part of an investigation. To satisfy this requirement, additional information such as the following may be sought:

- Volume of funds flowing through the account;
- Origin of the funds;
- Form in which the funds were offered or withdrawn e.g. cash, cheque;
- Identity of the person undertaking the transaction;
- Form of instruction and authority; and
- Name and address of the counterparty.

Financial institutions should document a formal anti-money laundering policy including evidence of compliance with provisions of section 8 of the Act relating to audit and training. At a minimum, records should be maintained on the following:

- (a) Details and contents of the training programme ;
- (b) Names of staff receiving training;
- (c) Dates of training sessions; and
- (d) Assessment of training.

It is important for institutions to ensure that the retrieval of relevant documentation is achieved within a reasonable time in order to comply with instructions issued by the Authority, High Court or regulator.

## **SECTION 6    REPORTING**

Financial institutions are required to submit reports to the Authority in compliance with any instructions issued by that body. See sub-sections 6(a) and 8(1)(c) of the Act. Appropriate reports must therefore be devised under the direction of the Authority.

As part of its internal control system, financial institutions should, at minimum, introduce management reports which, depending on the nature of each institution's operations, cover the following:

- (a) Cash volumes by branch;
- (b) Wire transfers by country;
- (c) Transactions secured by cash;
- (d) Large transaction reports (i.e. for transactions exceeding BDS\$10,000 or its foreign currency equivalent);
- (e) Suspicious transaction reports.

Appropriate information systems must therefore be in place to facilitate such reporting.

### **6.01    Large Transaction Reporting**

Financial institutions must establish and maintain reporting procedures to ensure compliance with Sections 9(1)(a) and 9(2) of the Act. As mentioned in section 4.0 of the guidelines, appropriate procedures should be developed to ensure the timely and effective delivery of internal reports.

Although not a requirement under the Act, the Central Bank recommends that financial institutions continue the practice of using large transaction reports to record and give special attention to transactions over the BDS\$10,000 threshold. However, institutions must be cognizant that such information can only be reported to

the Authority under sub-section 8(1)(b) of the Act which deals with suspicious transactions and sub-section 8(1)(c). Where such a report is being made, the Act does not allow an institution to notify the customer as this may constitute an offence under sub-section 22(1) of the Act. To this extent, the internal procedures and forms adopted by institutions to record large transactions must comply with the Act and should not for example require the customer's written consent to disclose information to the Authority.

Where a financial institution has developed a business relationship with a customer and determines that the nature of the business generates legitimate transactions in excess of the BDS\$10,000 threshold, then completion of a declaration form will not always be necessary. Institutions should clearly document their policy for the granting of such internal reporting waivers including the qualifying criteria for exemption, officers responsible for preparing and authorizing exemptions, basis for establishing threshold limits, review cycle of exempt customers and procedures for processing transactions. Each institution is required to maintain authorized lists of exempt customers showing threshold limits established in each case.

A specimen large transaction reporting format appears at **Appendix 8**.

## **6.02 Suspicious Transaction Reporting**

If a financial institution suspects that any transaction by a customer may involve proceeds of crime or is of an unusual nature, they must report their suspicions to the Authority forthwith. (See Sub-section 8(1)(b) of the Act). Consequently, appropriate internal reporting to the compliance officer must therefore be in place.

A suspicious activity is often one which is inconsistent in amount and origin with a customer's known, legitimate business or personal activities. The first step to recognition is knowing enough of the customer's business to recognise that a transaction, or series of transactions, is unusual. Examples of suspicious transactions appear at **Appendix 9**.

A record should be kept of all internal reports to management and reports made by the financial institution to the Authority. In the event that a financial institution declines to establish a business relationship with a prospective customer or to undertake a business transaction because of inadequate identification or documentation, a report should be sent to the Authority.

Reports should be in the format determined by the Authority (**see Appendix 10**) and addressed to:

**The Director**  
**Anti-Money Laundering Authority**  
**P.O. Box 1372**  
**Bridgetown**  
**Barbados**

Financial institutions, their directors and employees, should not warn their customers when information on suspicious activities relating to them is being reported to the law enforcement authorities. This may constitute an offence under sub-section 22(1) of the Act.

Financial institutions that report their suspicions, should follow the instructions from and otherwise cooperate fully with the Authority and law enforcement authorities in accordance with sub-sections 6(d) and 8(1)(c) of the Act.

## SECTION 7 TRAINING AND AWARENESS

An appropriate training programme should be developed in accordance with the institution's size, resources and type of operation. This should formally documented and form part of the anti-money laundering policy document.

Sub-section 6(c) of the Act states that the Authority will "establish training requirements and provide such training for any financial institution in respect of the business transaction record keeping and reporting obligations..." It is a legal requirement for financial institutions to comply with these requirements – sub-section 8(1)(f) and for financial institutions to provide their employees with appropriate training in the recognition and handling of money laundering transactions - sub-section 10(b).

All directors and employees should be aware of the Act and anti-money laundering guidelines. There may be a tendency to concentrate training efforts on front line staff but financial institutions should be cognizant of the fact that criminal activity may impact on various products and services throughout their operations.

Training programs should be tailored for various audiences including:

- (a) Front-line staff (e.g. tellers, customer service representatives, branch management);
- (b) Wire transfer employees;
- (c) Loans officers;
- (d) Accounting staff;
- (e) Internal audit;
- (f) Compliance officer(s);
- (g) Senior management and directors; and
- (h) New employees.

Training topics should generally cover:

- Laws and guidelines;
- Policies and procedures;
- Know-your-customer requirements;
- Know-your-business relationships;
- The identification of possible types of suspicious activities in all departments;
- Case studies of traditional schemes and new money laundering “typologies”;
- Reporting procedures; and
- Personal obligation and liability under the Act.

Financial institutions should ensure that the compliance officer(s) receive in-depth training on all aspects of the legislation and regulatory framework. Specific training should include:

- Policies and procedures to prevent money laundering;
- Customer identification, record keeping and other procedures;
- Recognition and handling of suspicious transactions; and
- New trends in criminal activity.

All training should be undertaken on a regular basis to ensure that there is a clear understanding of and adherence to internal policies and procedures as well as laws and guidelines.

## CONCLUSION

The exact size of money laundering worldwide is unknown - in 1996, a range of US\$ 590 billion to US\$1.5 trillion was suggested. Despite the inability to accurately measure its size, money laundering is recognized as a threat of international proportions. Such unwanted criminal activity can have severe economic repercussions on Barbados' economy. It is therefore critical that our jurisdiction enforces strict measures to combat money laundering.

While the Authority is the body charged with the responsibility of coordinating this fight, the battle must be supported by all of the major players in our financial sector. Financial institutions are likely to remain the focus of anti-money laundering attention, however the enormity of this threat reinforces the need for a broad-based defense for the sake of national interest.

**APPENDIX 1**  
**FATF MEMBER COUNTRIES**

Argentina	Italy
Australia	Japan
Austria	Luxembourg
Brazil	Mexico
Belgium	Kingdom of the Netherlands
Canada	New Zealand
Denmark	Norway
European Commission	Portugal
Finland	Singapore
France	Spain
Germany	Sweden
Greece	Switzerland
Gulf Co-operation Council	Turkey
Hong Kong, China	United Kingdom
Iceland	United States
Ireland	

**OBSERVER BODIES AND ORGANISATIONS**

Asia / Pacific Group on Money Laundering  
Caribbean Financial Action Task Force  
Council of Europe PC-R-EV Committee  
Eastern and Southern Africa Anti-Money Laundering Group  
Intergovernmental Task Force against Money Laundering in Africa

Further information can be obtained from the FATF at <http://www.fatf.oecd.org/fatf>



## APPENDIX 2

### THE FORTY RECOMMENDATIONS

#### Introduction

The Financial Action Task Force on Money Laundering (FATF) is an inter-governmental body whose purpose is the development and promotion of policies to combat money laundering - the processing of criminal proceeds in order to disguise their illegal origin. These policies aim to prevent such proceeds from being utilised in future criminal activities and from affecting legitimate economic activities.

The FATF currently consists of 29 countries<sup>1</sup> and two international organisations<sup>2</sup>. Its membership includes the major financial centre countries of Europe, North and South America, and Asia. It is a multi-disciplinary body - as is essential in dealing with money laundering - bringing together the policy-making power of legal, financial and law enforcement experts.

This need to cover all relevant aspects of the fight against money laundering is reflected in the scope of the Forty FATF Recommendations - the measures which the Task Force have agreed to implement and which all countries are encouraged to adopt. The Recommendations were originally drawn up in 1990. In 1996 the forty Recommendations were revised to take into account the experience gained over the last six years and to reflect the changes which have occurred in the money laundering problem<sup>3</sup>.

These Forty Recommendations set out the basic framework for anti-money laundering efforts and they are designed to be of universal application. They cover the criminal justice system and law enforcement; the financial system and its regulation, and international co-operation.

It was recognised from the outset of the FATF that countries have diverse legal and financial systems and so all cannot take identical measures. The Recommendations are therefore the principles for action in this field, for countries to implement according to their particular circumstances and constitutional frameworks allowing countries a measure of flexibility rather than prescribing every detail. The measures are not particularly complex or difficult, provided there is the political will to act. Nor do they compromise the freedom to engage in legitimate transactions or threaten economic development.

Footnote:

1 Reference in this document to "countries" should be taken to apply equally to "territories" or "jurisdictions". The twenty-nine FATF member countries and governments are: Argentina; Australia; Austria; Belgium; Brazil; Canada; Denmark; Finland; France; Germany; Greece; Hong Kong, China; Iceland; Ireland; Italy; Japan; Luxembourg; Mexico; the Kingdom of the Netherlands; New Zealand; Norway; Portugal; Singapore; Spain; Sweden; Switzerland; Turkey; the United Kingdom; and the United States.

2 The two international organisations are: the European Commission and the Gulf Cooperation Council.

3 During the period 1990 to 1995, the FATF also elaborated various Interpretative Notes which are designed to clarify the application of specific Recommendations. Some of these Interpretative Notes have been updated in the Stocktaking Review to reflect changes in the Recommendations. The FATF adopted a new Interpretative Note

relating to Recommendation 15 on 2 July 1999.

FATF countries are clearly committed to accept the discipline of being subjected to multilateral surveillance and peer review. All member countries have their implementation of the Forty Recommendations monitored through a two-pronged approach: an annual self-assessment exercise and the more detailed mutual evaluation process under which each member country is subject to an on-site examination. In addition, the FATF carries out cross-country reviews of measures taken to implement particular Recommendations.

These measures are essential for the creation of an effective anti-money laundering framework.

## **GENERAL FRAMEWORK OF THE RECOMMENDATIONS**

### **Recommendation 1**

Each country should take immediate steps to ratify and to implement fully, the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention).

### **Recommendation 2**

Financial institution secrecy laws should be conceived so as not to inhibit implementation of these recommendations.

### **Recommendation 3**

An effective money laundering enforcement program should include increased multilateral co-operation and mutual legal assistance in money laundering investigations and prosecutions and extradition in money laundering cases, where possible.

## **ROLE OF NATIONAL LEGAL SYSTEMS IN COMBATING MONEY LAUNDERING**

### **Scope of the Criminal Offence of Money Laundering**

#### **Recommendation 4**

Each country should take such measures as may be necessary, including legislative ones, to enable it to criminalise money laundering as set forth in the Vienna Convention. Each country should extend

the offence of drug money laundering to one based on serious offences. Each country would determine which serious crimes would be designated as money laundering predicate offences.

### **Recommendation 5**

As provided in the Vienna Convention, the offence of money laundering should apply at least to knowing money laundering activity, including the concept that knowledge may be inferred from objective factual circumstances.

### **Recommendation 6**

Where possible, corporations themselves - not only their employees - should be subject to criminal liability.

## **Provisional Measures and Confiscation**

### **Recommendation 7**

Countries should adopt measures similar to those set forth in the Vienna Convention, as may be necessary, including legislative ones, to enable their competent authorities to confiscate property laundered, proceeds from, instrumentalities used in or intended for use in the commission of any money laundering offence, or property of corresponding value, without prejudicing the rights of bona fide third parties.

Such measures should include the authority to: (1) identify, trace and evaluate property which is subject to confiscation; (2) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; and (3) take any appropriate investigative measures.

In addition to confiscation and criminal sanctions, countries also should consider monetary and civil penalties, and/or proceedings including civil proceedings, to void contracts entered into by parties, where parties knew or should have known that as a result of the contract, the State would be prejudiced in its ability to recover financial claims, e.g. through confiscation or collection of fines and penalties.

## **ROLE OF THE FINANCIAL SYSTEM IN COMBATING MONEY LAUNDERING:**

## **Recommendation 8**

Recommendations 10 to 29 should apply not only to banks, but also to non-bank financial institutions. Even for those non-bank financial institutions which are not subject to a formal prudential supervisory regime in all countries, for example bureaux de change, governments should ensure that these

institutions are subject to the same anti-money laundering laws or regulations as all other financial institutions and that these laws or regulations are implemented effectively.

## **Recommendation 9**

The appropriate national authorities should consider applying Recommendations 10 to 21 and 23 to the conduct of financial activities as a commercial undertaking by businesses or professions which are not financial institutions, where such conduct is allowed or not prohibited. Financial activities include, but are not limited to, those listed in the attached annex. It is left to each country to decide whether special situations should be defined where the application of anti-money laundering measures is not necessary, for example, when a financial activity is carried out on an occasional or limited basis.

## **Customer Identification and Record Keeping Rules**

### **Recommendation 10**

Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names: they should be required (by law, by regulations, by agreements between supervisory authorities and financial institutions or by self-regulatory agreements among financial institutions) to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, performing large cash transactions).

In order to fulfil identification requirements concerning legal entities, financial institutions should, when necessary, take measures:

- (i) to verify the legal existence and structure of the customer by obtaining either from a public register or from the customer or both, proof of incorporation, including information concerning the customer's name, legal form, address, directors and provisions regulating the power to bind the entity.

(ii) to verify that any person purporting to act on behalf of the customer is so authorised and identify that person.

### **Recommendation 11**

Financial institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted if there are any doubts as to whether these clients or customers are acting on their own behalf, for example, in the case of domiciliary companies (i.e. institutions, corporations, foundations, trusts, etc. that do not conduct any commercial or manufacturing business or any other form of commercial operation in the country where their registered office is located).

### **Recommendation 12**

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

Financial institutions should keep records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the account is closed. These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations.

### **Recommendation 13**

Countries should pay special attention to money laundering threats inherent in new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

## **Increased Diligence of Financial Institutions**

### **Recommendation 14**

Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.

### **Recommendation 15**

If financial institutions suspect that funds stem from a criminal activity, they should be required to report promptly their suspicions to the competent authorities.

### **Recommendation 16**

Financial institutions, their directors, officers and employees should be protected by legal provisions from criminal or civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in

good faith to the competent authorities, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

### **Recommendation 17**

Financial institutions, their directors, officers and employees, should not, or, where appropriate, should not be allowed to, warn their customers when information relating to them is being reported to the competent authorities.

### **Recommendation 18**

Financial institutions reporting their suspicions should comply with instructions from the competent authorities.

### **Recommendation 19**

Financial institutions should develop programs against money laundering. These programs should include, as a minimum :

- (i) the development of internal policies, procedures and controls, including the designation of compliance officers at management level, and adequate screening procedures to ensure high standards when hiring employees;
- (ii) an ongoing employee training programme;
- (iii) an audit function to test the system.

### **Measures to Cope with the Problem of Countries with No or Insufficient Anti-Money Laundering Measures**

## **Recommendation 20**

Financial institutions should ensure that the principles mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply these Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the mother institution should be informed by the financial institutions that they cannot apply these Recommendations.

## **Recommendation 21**

Financial institutions should give special attention to business relations and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply these Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.

## **Other Measures to Avoid Money Laundering**

### **Recommendation 22**

Countries should consider implementing feasible measures to detect or monitor the physical cross-border transportation of cash and bearer negotiable instruments, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements.

### **Recommendation 23**

Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering cases, subject to strict safeguards to ensure proper use of the information.

### **Recommendation 24**

Countries should further encourage in general the development of modern and secure techniques of money management, including increased use of checks, payment cards, direct deposit of salary checks, and book entry recording of securities, as a means to encourage the replacement of cash

transfers.

### **Recommendation 25**

Countries should take notice of the potential for abuse of shell corporations by money launderers and should consider whether additional measures are required to prevent unlawful use of such entities.

## **Implementation and Role of Regulatory and Other Administrative Authorities**

### **Recommendation 26**

The competent authorities supervising banks or other financial institutions or intermediaries, or other competent authorities, should ensure that the supervised institutions have adequate programs to guard against money laundering. These authorities should co-operate and lend expertise spontaneously or on request with other domestic judicial or law enforcement authorities in money laundering investigations and prosecutions.

### **Recommendation 27**

Competent authorities should be designated to ensure an effective implementation of all these Recommendations, through administrative supervision and regulation, in other professions dealing with cash as defined by each country.

### **Recommendation 28**

The competent authorities should establish guidelines which will assist financial institutions in detecting suspicious patterns of behaviour by their customers. It is understood that such guidelines must develop over time, and will never be exhaustive. It is further understood that such guidelines will primarily serve as an educational tool for financial institutions' personnel.

### **Recommendation 29**

The competent authorities regulating or supervising financial institutions should take the necessary legal or regulatory measures to guard against control or acquisition of a significant participation in financial institutions by criminals or their confederates.

## **STRENGTHENING OF INTERNATIONAL CO-OPERATION**

## **Administrative Co-operation**

### ***Exchange of General Information***

#### **Recommendation 30**

National administrations should consider recording, at least in the aggregate, international flows of cash in whatever currency, so that estimates can be made of cash flows and reflows from various sources abroad, when this is combined with central bank information. Such information should be made available to the International Monetary Fund and the Bank for International Settlements to facilitate international studies.

#### **Recommendation 31**

International competent authorities, perhaps Interpol and the World Customs Organisation, should be given responsibility for gathering and disseminating information to competent authorities about the latest developments in money laundering and money laundering techniques. Central banks and bank regulators could do the same on their network. National authorities in various spheres, in consultation with trade associations, could then disseminate this to financial institutions in individual countries.

### ***Exchange of Information Relating to Suspicious Transactions***

#### **Recommendation 32**

Each country should make efforts to improve a spontaneous or "upon request" international information exchange relating to suspicious transactions, persons and corporations involved in those transactions between competent authorities. Strict safeguards should be established to ensure that this exchange of information is consistent with national and international provisions on privacy and data protection.

## **Other Forms of Co-operation**

### ***Basis and means for co-operation in confiscation, mutual assistance and extradition.***

#### **Recommendation 33**

Countries should try to ensure, on a bilateral or multilateral basis, that different knowledge standards in national definitions -- i.e. different standards concerning the intentional element of the infraction -- do not affect the ability or willingness of countries to provide each other with mutual legal assistance.

### **Recommendation 34**

International co-operation should be supported by a network of bilateral and multilateral agreements and arrangements based on generally shared legal concepts with the aim of providing practical measures to affect the widest possible range of mutual assistance.

### **Recommendation 35**

Countries should be encouraged to ratify and implement relevant international conventions on money laundering such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.

## **Focus of Improved Mutual Assistance on Money Laundering Issues**

### **Recommendation 36**

Co-operative investigations among countries' appropriate competent authorities should be encouraged. One valid and effective investigative technique in this respect is controlled delivery related to assets known or suspected to be the proceeds of crime. Countries are encouraged to support this technique, where possible.

### **Recommendation 37**

There should be procedures for mutual assistance in criminal matters regarding the use of compulsory measures including the production of records by financial institutions and other persons, the search of persons and premises, seizure and obtaining of evidence for use in money laundering investigations and prosecutions and in related actions in foreign jurisdictions.

### **Recommendation 38**

There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate proceeds or other property of corresponding value to such proceeds, based on money laundering or the crimes underlying the laundering activity. There should also be arrangements for co-ordinating seizure and confiscation proceedings which may include the sharing of confiscated assets.

### **Recommendation 39**

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country. Similarly, there should be arrangements for co-ordinating seizure and confiscation proceedings which may include the sharing of confiscated assets.

#### **Recommendation 40**

Countries should have procedures in place to extradite, where possible, individuals charged with a money laundering offence or related offences. With respect to its national legal system, each country should recognise money laundering as an extraditable offence. Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgements, extraditing their nationals, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

#### **Annex to Recommendation 9: List of Financial Activities undertaken by business or professions which are not financial institutions**

1. Acceptance of deposits and other repayable funds from the public.
2. Lending<sup>1</sup>.
3. Financial leasing.
4. Money transmission services.
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques and bankers' drafts.)
6. Financial guarantees and commitments.
7. Trading for account of customers (spot, forward, swaps, futures, options) in:
  - (a) Money market instruments (cheques, bills, CDs, etc);
  - (b) Foreign exchange;
  - (c) Exchange, interest rate and index instruments;
  - (d) Transferable securities;
  - (e) Commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
9. Individual and collective portfolio management.
10. Safekeeping and administration of cash or liquid securities on behalf of clients.
11. Life insurance and other investment related insurance.
12. Money changing.

**Footnote:** \* Including *inter alia*: consumer credit; mortgage credit; factoring, with or without recourse and finance of commercial transactions (including forfaiting).

## APPENDIX 3

### CFATF MEMBER COUNTRIES

Anguilla	Jamaica
Antigua & Barbuda	Montserrat
Aruba	Netherlands Antilles
Bahamas	Nicaragua
Barbados	Panama
Belize	St. Kitts & Nevis
Bermuda	St. Lucia
British Virgin Islands	St. Vincent & the Grenadines
Cayman Islands	Suriname
Costa Rica	Trinidad & Tobago
Dominican Republic	Turks & Caicos Islands
Grenada	Venezuela
Guatemala	
Guyana	

### CO-OPERATING AND SUPPORTING NATIONS

Canada  
France  
Netherlands  
Spain  
United Kingdom  
United States of America

### OBSERVERS

Asia/Pacific Group Secretariat	FATF Secretariat
Caribbean Customs and Law Enforcement Council	UN Global Programme on Money Laundering
Caribbean Development Bank	Inter-American Development Bank
CARICOM	Interpol
CARIFORUM	Offshore Group of Banking Supervisors
Commonwealth Secretariat	Organization of American States /
European Commission	Inter-American Drug Abuse Control Commission
	United Nations Office for Drug Control and Crime Prevention

Further information can be obtained from the CFATF at [www.cfatf.org](http://www.cfatf.org)

## APPENDIX 4

### THE NINETEEN RECOMMENDATIONS

#### Anti-Money Laundering Authority

1. Adequate resources need to be dedicated to fighting money laundering. In countries where experience in combating money laundering is limited, there need to be competent authorities that specialize in money laundering investigations and prosecutions and related forfeiture actions, advise financial institutions and regulatory authorities on anti-money laundering measures, and receive and evaluate suspicious transaction information from financial institutions and regulators and currency reports which are filed by individuals or institutions.

#### Crime of Money Laundering

2. Consistent with recommendation 5 of the Financial Action Task Force and recognizing that the objectives of combating money laundering are shared by CFATF members, each country in determining for itself what crimes ought to constitute predicate offences, should be fully aware of the practical evidentiary complications that may arise if money laundering is made an offence only with respect to certain very specific predicate offences.
3. In accordance with the Vienna Convention, each country should, subject to its constitutional principles and the basic concepts of its legal system, criminalize conspiracy or association to engage in, and aiding and abetting drug trafficking, money laundering and other serious offences and subject such activities to stringent criminal sanctions.
4. When criminalizing money laundering, the national legislature should consider:
  - a. extend money laundering predicate offences beyond narcotics trafficking to include all serious crimes;
  - b. whether money laundering should only qualify as an offence in cases where the offender actually knew that he was dealing with funds derived from crime or whether it should also qualify as an offence in cases where the offender ought to have known that this was the case;
  - c. whether it should be relevant that the predicate offence may have been committed outside the territorial jurisdiction of the country where the laundering occurred;
  - d. whether it is sufficient to criminalize the laundering of illegally obtained funds, or

whether other property that may serve as a means of payment should also be covered.

5. Where it is not otherwise a crime, countries should consider enacting statutes that criminalize the knowing payment, receipt or transfer, or attempted payment, receipt or transfer of property known to represent the proceeds of drug trafficking, serious crimes or money laundering where the recipient of the property is a public official, political candidate, or political party. In countries where it is already a crime, countries should consider the imposition of enhanced punishment or other sanctions, such as forfeiture of office.

### **Privilege**

6. The fact that a person acting as a financial advisor or nominee is an attorney, accountant, stockbroker or other professional, should not in and of itself be sufficient reason for such person to invoke an attorney-client privilege, or any other confidentiality clauses.

### **Confiscation**

7. Confiscation measures should provide for the authority to seize, freeze, and confiscate, at the request of a foreign state, property in the jurisdiction in which such property is located regardless of whether the owner of the property or any persons who committed the offence making the property subject to confiscation are present or have ever been present within the jurisdiction.
8. Countries should provide for the possibility of confiscating any property that represents assets that have been directly or indirectly derived from drug offences or related money laundering offences (property confiscation), and may also provide for a system of pecuniary sanctions based on an assessment of the value of assets that have been directly or indirectly derived from such offences. In the latter case, the pecuniary sanctions concerned might be recoverable from any asset of the convicted person that may be available (value confiscation).
9. Confiscation measures may provide that all or part of any property confiscated be transferred directly for use by competent authorities, or be sold and the proceeds of such sales deposited into a fund dedicated to the use by competent authorities in anti-narcotics and anti-money laundering efforts.
10. Confiscation measures should also apply to narcotic drugs and psychotropic substances, precursor and essential chemicals, equipment and materials used or destined for the illicit manufacture, preparation, distribution and use of narcotic drugs and psychotropic substances.

## **Administrative Authorities**

11. In order to implement effectively the recommendations of the Financial Action Task Force, each country should have a system that provides for bank and other financial institution supervision, including:
  - 1) licensing of all banks, including offices, branches, and agencies of foreign banks whether or not they take deposits or otherwise do business in the country (so-called offshore shell banks), and
  - 2) the periodic examination of institutions by authorities to ensure that the institutions have adequate anti-money laundering programs in place and are following the implementation of other recommendations of the Financial Action Task Force.

Similarly, in order to implement the recommendation of the Financial Action Task Force, there needs to be effective regulation, including licensing and examination, of institutions and businesses such as services that make them vulnerable to money laundering.

12. Countries need to ensure that there are adequate border procedures for inspecting merchandise and carriers, including private aircraft, to detect illegal drug and currency shipments.

## **Record-keeping**

13. In order to ensure implementation of the recommendations of the Financial Action Task Force, countries should apply appropriate administrative, civil, or criminal sanctions to financial institutions and also businesses or professions which are not financial institutions that fail to maintain records for the required retention period. Financial institution supervisory authorities as well as supervisory authorities for businesses and professions which are not financial institutions must take special care to ensure that adequate records are maintained.

## **Currency Reporting**

14. Countries should consider the feasibility and utility of a system that requires the reporting of large amounts of currency over a certain specified amount received by businesses other than financial institutions either in one transaction or in a series of related financial transactions. These reports would be analyzed routinely by competent authorities in the same manner as any currency report filed by financial institutions. Large cash purchases of property and services such as real estate and aircraft are frequently made by drug traffickers and money launderers and, consequently, as of similar interest to law enforcement. Civil and criminal sanctions would apply to businesses and persons who fail to file or falsely file reports or structure transactions with the intent to evade the reporting requirements.

### **Administrative Co-operation**

15. In furtherance of recommendation 30 of the Financial Action Task Force, information acquired about international currency flows should be shared internationally and disseminated, if possible through the services of appropriate international or regional organizations, or on existing international networks. Special agreements may also be concluded for this purpose.
16. Member States of the OAS should consider signing the OAS Convention on Extradition, concluded at Caracas on February 25, 1981.
17. Each country should endeavour to ensure that its laws and other measures regarding drug trafficking and money laundering, and bank regulation as it pertains to money laundering, are to the greatest extent possible as effective as the laws and other measures of all other countries in the region.

### **Training and Assistance**

18. As a follow-up, there should be regular meetings among competent judicial, law enforcement, and supervisory authorities of the countries of the Caribbean and Central American region in order to discuss experience in the fight against money laundering and emerging trends and techniques.
19. In order to enable countries with small economies and limited resources to develop appropriate money laundering prevention programs, other countries should consider widening the scope of their international technical assistance programs, and to pay particular attention to the need of training and otherwise strengthening the quality and preserving the integrity of judicial, legal and law enforcement systems.



## APPENDIX 5

### BASLE STATEMENT OF PRINCIPLES

#### I. Purpose

Banks and other financial institutions may unwittingly be used as intermediaries for the transfer or deposit of money derived from criminal activity. The intention behind such transactions is often to hide the beneficial ownership of funds. The use of the financial system in this way is of direct concern to police and other law enforcement agencies; it is also a matter of concern to banking supervisors and banks' managements, since public confidence in banks may be undermined through their association with criminals.

This Statement of Principles is intended to outline some basic policies and procedures that banks' managements should ensure are in place within their institutions with a view to assisting in the suppression of money-laundering through the banking system, national and international. The Statement thus sets out to reinforce existing best practices among banks and, specifically, to encourage vigilance against criminal use of the payments system, implementation by banks of effective preventive safeguards, and cooperation with law enforcement agencies.

#### II. Customer Identification

With a view to ensuring that the financial system is not used as a channel for criminal funds, banks should make reasonable efforts to determine the true identity of all customers requesting the institution's services. Particular care should be taken to identify the ownership of all accounts and those using safe-custody facilities. All banks should institute effective procedures for obtaining identification from new customers. It should be an explicit policy that significant business transactions will not be conducted with customers who fail to provide evidence of their identity.

#### III. Compliance with Laws

Banks' management should ensure that business is conducted in conformity with high ethical standards and that laws and regulations pertaining to financial transactions are adhered to. As regards transactions executed on behalf of customers, it is accepted that banks may have no means of knowing whether the transaction stems from or forms part of criminal activity. Similarly, in an international context it may be difficult to ensure that cross-border transactions on behalf of customers are in compliance with the regulations of another country. Nevertheless, banks should not set out to offer services or provide active

assistance in transactions which they have good reason to suppose are associated with money-laundering activities.

#### **IV. Cooperation with Law Enforcement Authorities**

Banks should cooperate fully with national law enforcement authorities to the extent permitted by specific local regulations relating to customer confidentiality. Care should be taken to avoid providing support or assistance to customers seeking to deceive law enforcement agencies through the provision of altered, incomplete or misleading information. Where banks become aware of facts which lead to the reasonable presumption that money held on deposit derives from criminal activity or that transactions entered into are themselves criminal in purpose, appropriate measures, consistent with the law, should be taken, for example, to deny assistance, sever relations with the customer and close or freeze accounts.

#### **V. Adherence to the Statement**

All banks should formally adopt policies consistent with the principles set out in this Statement and should ensure that all members of their staff concerned, wherever located, are informed of the bank's policy in this regard. Attention should be given to staff training in matters covered by the Statement. To promote adherence to these principles, banks should implement specific procedures for customer identification and for retaining internal records of transactions. Arrangements for internal audit may need to be extended in order to establish an effective means of testing for general compliance with the Statement.

Further information can be obtained from at [www.bis.org](http://www.bis.org)





APPENDIX 7

IDENTIFICATION EXCEPTION (SPECIMEN)

DATE OF TRANSACTION:

1. EXEMPT CUSTOMER NAME (last ,first, middle) OR BUSINESS
2. TRADING NAME
3. PERSON COMPLETING TRANSACTION (last , first, middle)
4. PERMANENT ADDRESS
5. BASIS FOR EXEMPTION „ FINANCIAL INSTITUTION (specify)  „ LINKED TRANSACTION DATE OF ORIGINAL TRANSACTION : EFFECTIVE DATE: REFERENCE # :
6. EFFECTIVE DATE OF EXEMPTION
7. AMOUNT OF TRANSACTION

DESCRIPTION / NATURE OF BUSINESS TRANSACTION:

- „ Deposit
- „ Draft/Money Order Purchase
- „ Currency Exchange
- „ Travellers Cheques Purchase
- „ Wire Transfer
- „ Credit/Debit Card
- „ ATM
- „ Other (Specify)

.....

TRANSACTION TAKEN BY  
(Signature & Title)

AUTHORISING OFFICER  
(Signature & Title)

COMPLIANCE OFFICE  
(Signature & Title)

**APPENDIX 8**

**LARGE TRANSACTION REPORT (SPECIMEN)**

**[NAME & ADDRESS OF FINANCIAL INSTITUTION]**

**DATE OF TRANSACTION:**

1. CUSTOMER NAME (last first, middle) OR BUSINESS		7. NAME OF PERSON CONDUCTING TRANSACTION ,if different from previous	
2. PERMANENT ADDRESS		8. PERMANENT ADDRESS	
3. DATE AND PLACE OF BIRTH		9. DATE AND PLACE OF BIRTH	
4. NATIONALITY		10. NATIONALITY	
5. OCCUPATION		11. OCCUPATION	
6. HOME TELEPHONE NUMBER WORK TELEPHONE NUMBER		12. HOME TELEPHONE NUMBER WORK TELEPHONE NUMBER	
13. A/C NUMBER			
14. AMOUNT OF TRANSACTION & CURRENCY:			
FORM OF VERIFICATION	ISSUER & DATE	NUMBER	
15. NATIONAL I.D.			
16. PASSPORT			
17. DRIVERS LICENCE			
18. SOCIAL SECURITY			
19. OTHER (Specify)			

DESCRIPTION / NATURE OF BUSINESS TRANSACTION:

- Deposit     
  Draft/Money Order Purchase     
  Currency Exchange     
  Travellers Cheques Purchase  
 Wire Transfer   
  Credit/Debit Card                     
  ATM   
  Other (Specify)

**Source of Funds:** .....

.....  
 .....

**Transaction Approved?**    Yes     No

If No, state reason: .....

OFFICER COMPLETING TRANSACTION  
(Signature & Title)

AUTHORISING / COMPLIANCE OFFICER  
(Signature & Title)

## APPENDIX 9

### EXAMPLES OF SUSPICIOUS TRANSACTIONS

Money laundering is a global and dynamic phenomenon. The Financial Action Task Force meets annually to discuss money laundering trends and methods (referred to as "typologies"). These examples of suspicious transactions are not exhaustive and financial institutions are advised to keep abreast of any developments that would assist in their fight against money laundering.

- (a) Customers whose transactions are in size, type or nature not in accordance with their apparent source of wealth.
- (b) Unusual large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.
- (c) Customers seeking to exchange large quantities of cash of low denomination notes for those of higher denomination.
- (d) Frequent exchange of cash into other currencies.
- (e) Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.
- (f) Large cash deposits using night safe facilities, thereby avoiding direct contact with staff of licensed financial institutions.
- (g) Customers whose explanation of the source of funds is unclear and who decline to provide a satisfactory explanation.
- (h) Matching of payments out with credits paid in cash on the same or previous day.
- (i) Large cash withdrawals from a previously dormant or inactive account.
- (j) Greater use of safety deposit facilities. The use of sealed deposit and withdraw packets.
- (k) Substantial increase in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client, company or trust accounts.
- (l) Large number of individuals making payments into the same account without adequate

explanation.

- (m) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.
- (n) Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to overseas account(s).
- (o) Frequent requests for travellers cheques, foreign currency drafts or other negotiable instruments.
- (p) Request to borrow against an asset held by a financial institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.
- (q) Customers introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent.
- (r) Use of letters of credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.
- (s) Unexplained electronic fund transfers by customers, foreign currency drafts or other negotiable instruments to be issued.
- (u) Frequent paying in of travellers cheques or foreign currency drafts particularly if originating from overseas.

APPENDIX 10

SUSPECT TRANSACTION REPORT

SUSPECT TRANSACTION REPORT

PLEASE WRITE IN BLOCK LETTERS

IMPORTANT: Complete using information obtained during normal course of the transaction. The report should be completed as soon as practicable AFTER the dealing, and a copy forwarded to: THE DIRECTOR ANTI-MONEY LAUNDERING AUTHORITY P.O. BOX 1372 Bridgetown, Barbados FACSIMILE NO. (246) 436-4756 Email: amla@sunbeach.net For urgent reporting – Tel. (246) 436-4734/5

PART A Identity of customers involved in transaction

PART B Name of account holder

(To be completed only if transaction was conducted on behalf of another person other than those mentioned in part A (Given names and surname)

CUSTOMER 1

- 1.: (Date of birth)
2.: (Address)
3.: (Nationality – if not Barbadian)
4.: (Occupation)
5.: (Date of birth)
6.: Type and number of affected accounts
7.: Particulars of ID, e.g. National ID no., bank account no.

- 8.: (Given names and surname)
9.: (Address)
10.: (Nationality – if not Barbadian)
11.: (Occupation)
12.: (Date of birth)
13.: Type and number of affected accounts
14.: Particulars of ID, e.g. National ID no., bank account no.

CUSTOMER 2 (if more than one customer at counter)

PART C Transaction details

1.: .....  
(Given names and surname)

2.: .....  
.....  
(Address)

3.: .....  
(Nationality – if not Barbadian)

4.: .....  
(Occupation)

5.: .....  
(Date of birth)

6.: Type and number of affected accounts  
.....  
.....

7.: Particulars of ID, e.g. National ID no., bank account no.  
.....

15.: Type of transaction (e.g. deposit, purchase travellers chq)  
.....

16: Date of transaction .....

17: Amount of transaction (\$BC) .....

18. If foreign currency involved, name .....

19. Cheque/transfer/money order/etc.  
.....  
(Name of drawer/Ordering customer)

.....  
(Name of payee/beneficiary)

20. Other bank involved (if applicable) – name/branch/country  
.....  
.....

# SUSPECT TRANSACTION REPORT

PLEASE WRITE IN BLOCK LETTERS

**IMPORTANT:** Complete using information obtained during normal course of the transaction. The report should be completed as soon as practicable AFTER the dealing, and a copy forwarded to:  
**THE DIRECTOR**  
**ANTI-MONEY LAUNDERING AUTHORITY**  
**P.O. BOX 1372 Bridgetown, Barbados**  
**FACSIMILE NO. (246) 436-4756**  
**Email: amla@sunbeach.net**  
For urgent reporting – Tel. (246) 436-4734/5