MONEY LAUNDERING

GUIDELINES FOR FINANCIAL INSTITUTIONS*

[ISSUED 9 SEPTEMBER 2002]

The Supervisory Authority for Money Laundering†
O.N.D.C.P. Headquarters
Camp Blizard
Coolidge
Antigua, West Indies
Telephone: (268) 562-3255
Fax: (268) 460-8818
email: ondcp@candw.ag

---

* Section 11(vii) of the Money Laundering (Prevention) Act 1996
† Section 10 of the Money Laundering (Prevention) Act 1996

FOREWORD

These Guidelines are issued by the Supervisory Authority pursuant to the MLPA in order to outline the requirements of the Antigua and Barbuda's money laundering laws, to assist financial institutions to comply with those requirements, and to provide a practical interpretation of those provisions. They are designed not simply as a repetition of statutory provisions, but as guidance on how to put those provisions into practice.

These guidelines are designed to reflect world wide trends in anti-money laundering practice which are directed to ensuring that those who provide financial and other high value services (who in Antigua and Barbuda are gradually being defined as financial institutions in order to bring them under the ambit of the MLPA) take all appropriate steps to inform themselves about developments in money laundering that might affect them; train their staff; adopt anti-money laundering policies; apply appropriate due diligence procedures to their customers and report those who engage in suspicious activities to my office.

It is recognized that for practice Guidelines to be effective, they need to be reviewed on a regular basis to reflect changing circumstances and experience and to provide additional clarification concerning matters where queries often arise. For this reason, these Guidelines have been prepared in loose-leaf form, and as is necessary, they shall be updated by the issuing of additional pages or substitute pages, which it is suggested be maintained in a binder. Ultimately it is intended to publish the guidelines on the internet.

Issued: 9 September 2002

……
Wrenford D. Ferrance
Supervisory Authority under the MLPA
Director ONDCP

Issued by:

The Supervisory Authority
(Section 10, Money Laundering (Prevention) Act 1996)
Office of National Drug and Money
Laundering Control Policy
Camp Blizard
Coolidge
Antigua, West Indies

Telephone: (268) 562-3255
(268) 462-5934

Fax: (268) 460-8818

Email: ondcp@candw.ag

Table of Contents

MONEY LAUNDERING — GUIDELINES FOR FINANCIAL INSTITUTIONS

INTRODUCTION

WHAT IS MONEY LAUNDERING?

(i) Money laundering is the process by which criminals attempt to conceal the illegal origin and illegitimate ownership of property and assets that are the fruits or proceeds of their criminal activities. If undertaken successfully, it also allows them to impliedly represent the proceeds of their crime as having a legitimate source, and thereby maintain control over those proceeds and dispose of them without hindrance, which, ultimately is the goal of crime committed for profit.

(ii) Money laundering is a global phenomenon that affects all countries to varying degrees. By its very nature it is a hidden activity. However, failure to prevent the laundering of the proceeds of crime permits criminals to benefit from their actions.

THE NEED TO COMBAT MONEY LAUNDERING

(iii) There has been a growing recognition in recent years that it is essential that criminals be prevented, whenever possible, from legitimising the proceeds of their criminal activities by converting funds from “dirty” to “clean”.

(iv) The ability to launder the proceeds of criminal activity through the financial system is vital to the success of criminal operations. Those involved need to exploit the facilities of the world’s financial sector businesses, which includes facilities in Antigua and Barbuda, if they are to benefit from the proceeds of their activities.

(v) The long term success of any of the world’s financial sectors depends on attracting and retaining legitimately earned funds. Criminally earned money is invariably transient in nature. It damages reputation and deters the honest investor. Financial institutions and financial businesses that become involved in a money laundering scandal will risk likely prosecution, the loss of their good market reputation, and damaging the reputation of Antigua and Barbuda as a safe and reliable financial jurisdiction.

(vi) Money laundering is often thought to be associated solely with deposit taking institutions and other credit institutions. Whilst the traditional deposit taking institution processes of receiving funds, providing money transfer systems and lending do offer a vital laundering mechanism, particularly in the initial conversion from cash, it should be recognised that products and services offered by other types of financial and non-financial sector businesses are also attractive to the launderer. The sophisticated launderer often involves many other unwitting accomplices such as:

- insurance companies
- money exchange and transmission services
- financial intermediaries
- accountants and attorneys-at-law
- surveyors and estate agents
- casinos (including internet gaming and sports betting businesses)
- company formation agents
- antique dealers, car dealers and others selling high value commodities and luxury goods

STAGES OF MONEY LAUNDERING

(vii) There is no one method of money laundering. Methods can range from the purchase and resale of a luxury item (e.g. a car or jewellery) to passing money through a complex international web of legitimate businesses and 'shell' companies *(i.e. those companies that primarily exist only as names legal entities without any trading or business activities).* Initially, however, in the case of drug trafficking and some other serious crimes, the proceeds usually take the form of cash that needs to enter the financial system by some means.

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

a) Placement - the physical disposal of *the initial* proceeds derived from illegal activity.

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

c) Integration – the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-

enter the financial system appearing as normal business funds.

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

(ix) Certain points of vulnerability have been identified in the laundering process which the money launderer finds difficult to avoid and where his activities are therefore more susceptible to being recognised, specifically:

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

Examples of Suspicious Transaction/Activity

(x) Appendix A to these Guidelines describes a number of potentially suspicious transactions and activities relating to cash transactions.

WHAT THE LAW REQUIRES

[Appendix B to these Guidelines contains a summary of the Antigua and Barbuda legislation]

(xi) This section focuses on the provisions of the Money Laundering (Prevention) Act 1996 (MLPA), which is the primary money laundering legislation, in relation to the requirements and conduct of financial institutions and their employees.

OFFENCES

(xii) The law makes it an offence for any person to obtain, conceal, retain, manage, or invest money or other property or bring such money or other property into Antigua and Barbuda if that person knows or has reasonable grounds to suspect is derived directly or indirectly from unlawful activity.

Assistance

(xiii) Assistance someone to engage in money laundering includes aiding, abetting, counseling and procuring, and conspiring with someone to commit the offence.

Tipping off

(xiv) It is also an offence for anyone who knows or suspects that an investigation into money laundering has been, is being, or is about to be conducted to inform someone else of that fact thereby prejudicing the investigation.

Failure to Report

(xv) It is an offence for a financial institution or its employees, staff, directors, owners or other authorized representatives to willfully fail to report suspicious transactions or to make a false or falsified report.

(xvi) In the case of customer services officer, internal reporting in accordance with procedures laid down by the employer will satisfy this requirement. Reports by customer service officers should be made to the compliance officer. Upon receipt of a report from a customer services officer, a Compliance Officer must assess the report to determine whether a suspicious transaction report should be made.

Customer Confidentiality

(xvii) The legislation protects those reporting in good faith any suspicions of money laundering from claims in respect of any alleged breach of client confidentiality (See section 26 of the Act).

MONEY LAUNDERING (PREVENTION) REGULATIONS 1999 ("The Regulations")

These regulations contain provisions relating to identification and record keeping procedures. They are currently the subject of review.

Further guidance on the operation of the regulations will be provided in future updates of the guidelines

Section 1

1 INTERNAL CONTROLS, POLICIES AND PROCEDURES

Responsibilities and Accountabilities

1.0 Financial institutions are required to establish clear responsibilities and accountabilities to ensure that policies, procedures and controls are introduced and maintained which deter criminals from using their facilities for money laundering, **thus ensuring that they comply with their obligations under the law**. It is difficult to achieve this objective unless a person within each financial institution is given responsibility for carrying out this function together with the necessary authority to carry it out. Institutions must therefore appoint a Compliance Officer to undertake this role. In addition, the Compliance officer will be the central point of contact with the Supervisory Authority.

1.1 The functions of the Compliance Officer shall be to:

(1) receive and vet suspicious activity reports from staff

(2) file suspicious transaction reports with the Supervisory Authority;

(3) develop an anti money laundering compliance programme;

(4) ensure that the anti money laundering compliance programme is enforced;

(5) coordinate training of staff in anti money laundering awareness, detection methods etc.

Recommended Procedures

1.2 All financial sector businesses operating within the jurisdiction of Antigua and Barbuda should:

I. Have comprehensive procedures relating to the identification of their customers and the verification of customer identity in most instances;

II. Have procedures for the prompt validation of suspicions and subsequent reporting to the Supervisory Authority;

III. Provide the Compliance Officer with the necessary access to systems and records to fulfil this requirement; and,

IV. Maintain close co-operation and liaison with the Supervisory Authority.

1.3 Financial institutions should make arrangements to verify, on a regular basis, compliance with policies, procedures, and controls relating to money laundering activities, in order to satisfy management that the requirement to maintain such procedures have been discharged. Larger financial institutions may wish to ask their internal audit or compliance departments to undertake this role, while smaller institutions may wish to introduce a regular review by management.

1.4 It is important that the procedures and responsibilities for monitoring compliance with and effectiveness of money laundering policies and procedures are clearly laid down by all financial institutions in the form of policy documents and internal procedural manuals.

Section 2

2 IDENTIFICATION PROCEDURES (DUE DILIGENCE)

2.1 DEPOSIT TAKING INSTITUTIONS‡

DEFINITIONS/EXPLANATIONS OF TERMS

2.1.1 The person or company whose identity must be established and, in some cases, verified is described as a **"customer"**.

An customer may be seeking to establish a business relationship with a deposit taking institution or may be an occasional customer undertaking a one off transaction. This can affect identification requirements.

A "**business relationship"** is any arrangement between the deposit taking institution and a customer the purpose of which is to facilitate the carrying out of transactions between the parties on a frequent, habitual or regular basis, and where the monetary value of dealings in the course of the arrangement is not known or capable of being ascertained at the outset. The opening of an account with a deposit taking institution should therefore be treated as forming a 'business relationship'.

A "**one off transaction"** means any transaction carried out other than in the course of an business relationship. For example, a single foreign currency transaction for a customer who does not have an account at the deposit taking institution concerned constitutes a one off transaction. A one off transaction is "significant" if it involves a sum equal to or greater than $EC10,000.

"KNOW YOUR CUSTOMER"

‡ See Appendix C, Nos. 1, 2, 4, 5, 7, 8, 9, 10, 12, 13, 15, 19

2.1.2 “Know your customer “ requirements consist of obtaining full particulars of the identity of customers (which may need to be verified in certain circumstances) and a sound knowledge of the purpose for which the customer is seeking to establish a business relationship with a financial institution. This knowledge needs to be applied to all dealings initiated by the customer. The extent to which such dealings appear not to ‘fit’ this knowledge base will become the basis of a financial institution’s suspicion about the customer which should then be reported to the Supervisory Authority.

2.1.3 The need for deposit taking institutions to “know your customers” is vital for the prevention of money laundering and underpins all other activities. If a customer has established an account under a false identity, he or she may be doing so for the purpose of defrauding the deposit taking institution itself or merely to ensure that they cannot be traced or linked to the proceeds of the crime that the institution is being used to launder.

2.1.4 When a business relationship is being established, the nature of the business that the customer expects to conduct with the deposit taking institution should be ascertained at the outset to show what might be expected as normal activity. In order to be able to judge whether a transaction is or is not suspicious, deposit taking institutions need to have a clear understanding of the legitimate business of their customers.

2.1.5 The procedures which deposit taking institutions adopt to comply with money laundering legislation will inevitably overlap with the prudential fraud prevention measures which they would undertake in order to protect themselves and their genuine customers. So far as lending is concerned, a deposit taking institution will naturally want to make specific checks on a customer’s credit-worthiness, employment and other income details. Such checks will often be very similar to identity checks undertaken for money laundering purposes.

What is Identity?

2.1.6 An individual’s identity comprises

(a) for persons:
- (i) name;
- (ii) other names used;
- (iii) residential address;
- (iv) country of citizenship;
- (v) date of birth.

(b) for incorporated entities:
- (i) name;

(ii) place of incorporation;
(iii) address of registered office;
(iv) name and address of local agent;
(v) names of directors, secretary, other office bearers;

Requirement to Identify Customers

2.1.7 Financial institutions must obtain particulars of the identity of all customers:

(a) if a relationship is conducted through an account – at the time the account is opened;
(b) if a relationship is conducted on the basis of a one off transaction – at the time the transaction occurs.

2.1.8 Any subsequent changes to the identity the customer of which the deposit taking institution becomes aware should be recorded as part of the know your customer process. Generally this would be undertaken as part of best practice and due diligence (i.e. for the deposit taking institution's own protection against fraud and bad debts), but it also serves for money laundering prevention.

WHEN IDENTITY MUST BE VERIFIED

2.1.9 Whenever a business relationship is to be established e.g. when an account is opened with a deposit taking institution, or a significant one-off transaction or series of linked transactions is undertaken the identity of the customer must be verified.

2.1.10 Once verification procedures have been satisfactorily completed and a business relationship has been established, no further verification of identity is required when transactions are subsequently undertaken for that customer as long as regular contact is maintained. When an existing customer closes one account and opens another there is no need to re-verify identity. Where a business relationship becomes inactive (no transactions for a year or more) a customer's identity should be re-verified in the event that the customer wishes to recommence business activity.

One off Transactions: Single or Linked

2.1.11 Verification of identity is not needed in the case of a single one-off transaction i.e. when the applicant is not expected to require further

services from the deposit taking institution concerned and when payment by, or to the applicant is less than EC$10,000.

2.1.12 However, verification procedures should be undertaken for linked transactions that together exceed the EC$10,000 limit, i.e. where in respect of two or more one-off transactions:

i. It appears at the outset to a person handling any of the transactions that the transactions are linked and that the aggregate amount of these transactions will amount to EC $10,000;

ii. At any later stage it comes to the attention of such a person that the transactions are linked and that the EC $10,000 limit has been reached.

For the purpose of these Guidelines, it is suggested that transactions, which are separated by an interval of three months or more, need not, in the absence of specific evidence to the contrary, be treated as linked.

Verification procedures should also be taken in respect of any transaction whether or not it exceeds EC$10,000 if the customer service officer becomes suspicious about the customer or the transaction (a suspicious transaction report should also be made in such circumstances).

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

Timing of Verification Requirements

2.1.14 What constitutes an acceptable time span for obtaining satisfactory verification of identity must be determined in light of all the circumstances including the nature of the business, the geographical location of the parties and whether it is practical to verify identity before commitments are entered into or money is deposited. Deposit taking institutions can start processing the business or application for account opening immediately, provided that it promptly takes appropriate steps to verify the customer's identity and does not transfer or pay any money out to a third party until the verification requirements have been satisfied. In preparing their procedures, deposit taking institutions will need to establish clear and consistent policies to deal with situations where satisfactory evidence of identity cannot be obtained. In some circumstances, the failure of an applicant to provide satisfactory

evidence of identity without adequate explanation may in itself lead to a suspicion that the investor is engaged in money laundering.

VERIFICATION PROCEDURES

Establishing satisfactory Evidence of Identity

2.1.15 A deposit taking institution should establish to its satisfaction that it is dealing with a real person or entity (natural, corporate or legal), and verify the identity of those persons who have power to operate any deposit taking institution or investment account. If funds to be deposited or invested are being supplied by or on behalf of a third party, it is essential to establish the identity of the third person (i.e. the underlying beneficiary).

2.1.16 In respect of joint personal accounts the name and address of all account holders should be verified in accordance with the procedures set out below.

IDENTITY VERIFICATION FOR PERSONAL CUSTOMERS

Personal Customers Resident in Antigua and Barbuda

2.1.17 The following information should be established or independently verified:

- True name and other names used by the customer;
- Correct permanent address, including telephone number

2.1.18 The date of birth is also important as an identifier in support of the name and is of particular value to law enforcement agencies in an investigation. In addition, obtaining a date of birth provides an extra safeguard if, for example, a forged or stolen passport or driving licence is used to confirm identity which bears a date of birth that is clearly inconsistent with the age of the person presenting the document

Documentary Evidence

2.1.19 Where an applicant is seen in person, their true name and other names used should be verified by reference to a document which has been obtained from a reputable source which bears a photograph. This would normally be a current valid passport, driver's licence or government issued identity card. That part of the document containing particulars of the person's identification should be copied and retained on the customer's file.

2.1.20 Because documents providing photographic evidence of identity need to be compared with the applicant's appearance, and to guard against the dangers of postal intercept and fraud, prospective customers should not be asked to send their original identity documents by post to a deposit taking institution. In the event that internal procedures require sight of a current passport or national identity card where there is no face to face contact, then a certified copy should be requested.

Other Searches and Enquiries

2.1.21 In addition to the name, it is important that the current permanent address is verified, as it is an integral part of identity. Satisfactory evidence can be obtained by undertaking a combination of the following checks:

- Checking the Register of Electors;
- Making a credit reference agency search;
- Requesting sight of a recent utility bill, tax bill, deposit taking institution statement (to guard against forged or counterfeit documents, care should be taken to check that the documents offered are originals);
- Checking a local telephone directory.

2.1.22 An introduction from a respected customer personally known to the Manager, or from a trusted member of staff, may assist the verification procedure but cannot replace it. Details of who initiated and authorised the introduction should be recorded on the customer's file. Directors/senior managers must not require or request other staff to breach account opening procedures as a favour to a customer.

Identity Verification of Minors, Students, the Elderly and Disabled People

[Note: Re Minors: this section applies only to deposit, savings and investment accounts, since minors are legally precluded from applying for mortgages and other loans.]

2.1.23 It is acknowledged that there will be circumstances when Antiguan and Barbudan residents, particularly young persons, the elderly and disabled people, may not be able to provide full documentary evidence of their identity, and where independent address verification is not possible. In such cases, a senior manager could authorise the opening of an account if he or she is satisfied with the circumstances but must record his or her authorisation on the

customer's file, and must also retain this information in the same manner and for the same period of time as other identification records.

2.1.24 It is important that young persons, elderly and disabled people, should not be precluded from opening deposit taking institution accounts merely because they cannot produce the preferred documents confirming their identity. Internal procedures should allow for such circumstances and should provide appropriate advice to account opening staff on how identity can be confirmed and what local checks can be made.

2.1.25 When opening accounts for students and other young people, the normal identification procedures, set out in the above paragraphs, should be followed as far as possible. Where such procedures would not be relevant, or do not provide satisfactory evidence of identity, verification could be obtained via the home address of the parent(s) or by making enquiries of the applicant's college or University. However, care should be taken at the commencement of the academic year before a student has taken up residence at the college, as registration frauds are known to occur at this time.

2.1.26 Under normal circumstances, a minor would be introduced to the deposit taking institution by a family member or guardian who has an existing relationship with the institution concerned. In cases where such a nominee opening account is not already known to the deposit taking institution, the identity of that nominee, or of any other person who will have control of the account, should be verified.

2.1.27 For accounts opened through a school related scheme, the school should be asked to provide the date of birth and permanent address of the pupil to complete standard account opening procedures.

Personal Accounts of Non Residents of Antigua and Barbuda

Face to Face Applications

2.1.28 For those prospective customers who are not normally resident in Antigua and Barbuda but who make face to face contact, passports or national identity cards will always be available and copies of those parts of such documents which contain particulars of a customer's identity should be obtained. It is impractical to set out detailed descriptions of various identity cards and passports that might be offered as evidence of identity by foreign nationals. In addition, deposit taking institutions should verify the identity and address of an applicant with a reputable credit or financial institution in the applicant's home country or country of residence. Alternatively, where a foreign national is temporarily resident in Antigua or Barbuda, reference might be made to an employer, learning institution, etc. to corroborate the applicant.

Executorship Accounts

2.1.29 Where an account is opened for the purpose of winding up the estate of a deceased person, the identity of the executor(s)/administrators of the estate should be verified in line with the requirements for other accounts, depending on the nature of the executors (i.e. whether personal, corporate or a firm of solicitors).

2.1.30 However, the identity of the executor or administrator should not normally need to be verified when payment from an established deposit taking institution in the deceased's name is being made to the executors or administrators in accordance with the Grant of Probate or Letters of Administration solely for the purpose of winding up the estate.

2.1.31 Payments to the underlying beneficiaries on the instructions of the executor or administrator may be made without additional verification requirements.

2.1.32 In the event that any suspicions are aroused concerning the nature or origin of assets comprising an estate that is being wound up, then a report of the suspicions should be made in accordance with the procedures set out in this document.

Power of Attorney

2.1.33 The authority to deal with assets under a Power of Attorney constitutes a business relationship and therefore, where appropriate, it may be advisable to check the identity of holders of powers of attorney or third party mandates. Records of all transactions undertaken in accordance with the Power of Attorney should be kept in accordance with procedures laid out in this document.

Non-Face to Face Verification: Non Residents of Antigua and Barbuda

2.1.34 For prospective non-resident customers who wish to open an account with a deposit taking institution *without face to face contact,* it will not be practical to seek sight of the original of a passport or national identity card. There are a number of alternative measures that can be taken

- a certified copy of the passport should be obtained;

- An account opening reference can be sought from a reputable credit or financial institution in the applicant's home country. Verification details should be requested

covering true name/s used, current permanent address, date of birth, and verification signature.

2.1.35 Particular care should be taken when relying on financial sector businesses from countries with substandard money laundering regulations to ensure that the customer's identity and current permanent address can be confirmed. Copies of relevant identity documents should be sought and retained in Antigua and Barbuda.

Internet and Cyberbanking

2.1.36 Internet banking adds a new dimension to the risks faced by financial institutions and opens up new mechanisms for fraud and money laundering because its use is largely unregulated.

2.1.37 Any deposit taking institution offering Internet banking facilities should implement procedures to identify and authenticate the customer, and should ensure that there is sufficient communication to confirm address and personal identity. Care should be taken to ensure that the same supporting documentation is obtained from Internet customers as for other non face to face customers.

2.1.38 Deposit taking institutions should consider regular monitoring of accounts opened on the Internet. Unusual transactions should be investigated and reported if suspicious.

IDENTITY VERIFICATION FOR INSTITUTIONS

Incorporated Entities

2.1.39 Copies of the following documents should be obtained in order to verify particulars of identification provided by corporate customers (whether registered onshore or offshore):

(a) certificate of incorporation;
(b) memorandum and articles of association;
(c) certificate showing the registered office of the corporation;
(d) company registration form showing particulars of current directors

Clubs and Societies

2.1.40 In the case of accounts to be opened for clubs or societies, a deposit taking institution should satisfy itself as to the legitimate purpose of the organisation by, for example, requesting sight of the constitution. The identity of all signatories should be verified and, when signatories change, care should be taken to ensure that the identity of new signatories is verified.

TRUST, NOMINEE AND FIDUCIARY ACCOUNTS

2.1.41 Trust, nominee and fiduciary accounts are a popular vehicle for criminals wishing to avoid the identification procedures and mask the origin of the criminal money they wish to launder.

2.1.42 In addition to the usual procedures relating to the identification of the account holder, measures must be taken to establish and verify the identity of the underlying beneficiary on whose behalf an applicant for business is acting. For trusts, this will generally mean being able to rely on an introduction certificate from a professional trustee or other regulated financial sector business, thereby creating a chain of responsibility. The trustees/nominees should therefore be asked to state from the outset the capacity in which they are operating or making the application. Sight of the original trust deed, and any subsidiary deed evidencing the appointment of current trustees, other should also be obtained. Any application to open an account or undertake a transaction on behalf of another without the applicant's identifying their trust or nominee capacity should be regarded as suspicious and should lead to further enquiries.

2.1.43 An important factor to avoid laundering via trust, nominee and fiduciary accounts is that information on the identity of the settlor and/or beneficial owner of the funds, who provided the funds, and of any controller or similar person having power to appoint or remove the trustees or fund managers and the nature and purpose of the trust must be available to law enforcement in the event of an enquiry. Deposit taking institutions should therefore obtain the identity of the underlying principals, in particular those who are supplying and have control of the funds.

"CLIENT ACCOUNTS" OPENED BY PROFESSIONAL INTERMEDIARIES

2.1.44 The above guidelines relating to trusts, nominees and fiduciaries apply to lawyers, accountants and other business intermediaries who may seek to establish accounts with financial institutions on behalf of their clients.

ACQUISITION OF ONE FINANCIAL SECTOR BUSINESS BY ANOTHER

2.1.45 When a deposit taking institution acquires the business and accounts of another financial sector company or firm, either in whole or as part of a portfolio (i.e. the mortgage book), it is not necessary for the identity of all existing customers to be re-identified, provided that all customer account records are acquired with the business and that due diligence enquiries do not give rise to doubt that the money laundering procedures previously adopted by the business that has been acquired have been fully satisfied in accordance with Antiguan and Barbudan requirements.

2.1.46 In the event that the money laundering procedures previously undertaken have not been in accordance with Antiguan and Barbudan requirements, or the procedures cannot be checked, or the customer records are not available to the acquiring deposit taking institution, verification of identity procedures will need to be undertaken for all transferred customers as soon as is practicable.

2. IDENTIFICATION PROCEDURES (DUE DILIGENCE)

2.2 INTERNET GAMING[§]

2.2.1 Internet gaming businesses, either casinos or sports betting operations, are a relatively new form of financial institution for Antigua and Barbuda. Insofar as they accept funds from customers for the purpose of opening 'player accounts' they are similar to the financial institutions for which guidelines are provided in 2.1. However, there are a number of differences which justify the creation of special guidelines for such financial institutions.

2.2.2 Internet gaming businesses are subject both to the provisions of the MLPA and to the Interactive Gaming and Interactive Wagering Regulations 2001 (IGIWR). The terms "player", "player accounts" and "licence holder" have the same meaning as is given to them in the IGIWR.

2.2.3 Section 1 of these Guidelines relating to the establishment of a compliance programme by financial institutions and paragraphs 2.1.1 – 2.1.8 relating to customer (player) identification apply to internet gaming businesses, save that all business transacted between a player and a licence holder must be conducted via a player account. Guidelines relating to one off transactions and linked one off transactions therefore do not apply.

VERIFICATION OF IDENTITY

[§] See Appendix C, No. 16

2.2.4 Regulation 127(a) of the IGIWR provides that no payment in excess of $US5,000 may be made from a player account unless satisfactory evidence of the player's age, place of residence and identity has been provided to the licence holder.

2.2.5 Satisfactory evidence of age, residence and identity consists of:

(a) Production to the licence holder of a photocopy of the relevant parts of an identification document issued by a government or government authority such as a passport, driver's licence or identity card;
(b) Satisfactory credit check or banking reference that does not produce any information inconsistent with that contained in subparagraph (a) or with any other particulars provided by the player at the time their player account was opened.

2.2.6 The information derived as a result of the verification procedures in paragraph 2.2.5 must confirm the age, residence and identity of the player.

2.2.7 Where incomplete or unsatisfactory evidence of identity is provided no payments should be made from the player account and the matter should be discussed with the Directorate of Gaming. If the failure to provide the necessary information raises a suspicion concerning the player a suspicious transaction report should also be filed with both the Supervisory Authority and the Directorate of Gaming.

PAYMENTS FROM PLAYERS

2.2.8 Licence holders may only accept payments by means of:

(a) credit or debit card;
(b) electronic transfer;
(c) wire transfer;
(d) cheque
(e) or by such other means as may, from time to time be approved by the Financial Sector Regulatory Commission.

2.2.9. Payments referred to in paragraph 2.2.8 should only be accepted if they are processed through properly established, reputable and well regulated financial institutions.

2.2.10 Licence holders may never receive payments from players in cash.

PAYMENTS TO PLAYERS

2.2.11 Payments to players should only be made to the address shown to be their residential address. Under no circumstances should payments be made to third parties or to jurisdictions other than the jurisdiction from which the stake money paid into the player's account was paid.

2.2.12 Payments to players for an amount exceeding $US 25,000 should be made the subject of a significant transaction report to the Supervisory Authority within 48 hours of the payment being made (IGIWR 125(d)).

2.2.13 Any attempt made by a player to structure** payments to avoid the reporting requirements in IGIWR 125(d) should be made the subject of a suspicious transaction report.

2.2.14 Licence holders should only make payments to players who hold accounts with them. Under no circumstances should they make payments (by way of set off etc.) to customers of other gaming companies.

** split payments into multiple amounts of less than $US25,000 but which, in aggregate amount to more than $US25,000, in order to avoid the reporting requirements.

Section 3

3 RECORD KEEPING

FORMAT AND RETRIEVAL OF RECORDS

Format of Records

3.1 It is recognised that financial institutions will find it necessary to rationalise their hard copy filing requirements. Most will have standard procedures which seek to reduce the volume and density of records which have to be stored, whilst still complying with statutory requirements. Retention may therefore be by way of: original documents; stored on microfiche; computerised; or, electronic form. However, the record retention requirements are the same regardless of the format in which they are kept or whether the transaction was undertaken by paper or electronic means. Documents held centrally must be capable of distinguishing between the transactions relating to different customers and of identifying where the transaction took place and in what form.

Records of transactions are required to be kept for six years after the date of the relevant transaction. Records relating to the establishment or operation of accounts must be kept for six years after the date the account was closed. (MLPA section 12)

Retrieval of Relevant Records

3.2 The Regulations do not state the location where relevant records should be kept but the overriding objective is for financial sector businesses to be able to retrieve relevant information without delay. Production Orders that are granted by the Court to an investigating officer under the Money Laundering (Prevention) Act 1996, as amended, will usually require that the information specified should be available within seven calendar days of the date of the service of the Order unless a longer period has been applied for by the investigating officer and included in the Court Order.

3.3 Financial sector businesses are asked to ensure that when original documents, which would normally have been destroyed (after the six year retention period has elapsed), are required for investigation purposes, they check that the destruction policy has actually been carried out before informing the law enforcement agency that the documents are not available.

Section 4

4 RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

RECOGNITION OF SUSPICIOUS ACTIVITIES

4.1 As the types of transaction which may be used by money launderers are almost unlimited, it is difficult to define suspicious transactions with any particularity. Suspicion is personal and subjective and falls far short of proof based on firm evidence. In order to develop a suspicion that a transaction may involve the proceeds of crime, a person is not expected to know the exact nature of the criminal offence involved or that the particular funds were definitely those arising from it.

4.2 Where there is a business relationship, a suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business activity for that type of account. Therefore, the first key to recognition is knowing enough about the customer and the customer's business to recognise that a transaction, or series of transactions, is unusual.

4.3 Questions that a financial institution might consider when determining whether an established customer's transaction is suspicious or not are:

- is the size of the transaction consistent with the normal activities of the customer?

- Is the transaction rational in the context of the customer's business or personal activities?

- Has the pattern of transactions conducted by the customer changed?

- Where the transaction is international in nature, and the client is based overseas, does the customer have any obvious reason for conducting business with Antigua and Barbuda? If the customer is based in Antigua and Barbuda is there any obvious reason for the customer conducting business overseas?

Examples of Suspicious Transactions

4.4 Examples of what might constitute suspicious transactions are given in Appendix A. These are not intended to be exhaustive and provide examples only of the most basic ways by which money may be laundered. However, identification of any of the types of transactions listed in Appendix A should be the catalyst for further investigation.

4.5 Sufficient guidance must be given to staff to enable them to recognize suspicious transactions. The type of situations giving rise to suspicions will depend on a financial institution's customer base and range of services and products. Financial institutions might also consider monitoring the types of transactions and circumstances that have given rise to suspicious transaction reports by staff, with a view to updating internal instructions and guidelines from time to time.

REPORTING OF SUSPICIOUS TRANSACTIONS

4.6 There is a statutory obligation on all financial institutions to report suspicions of money laundering to the Supervisory Authority. (See Section 13 of the Money Laundering (Prevention) Act 1996).

4.7 All financial Institutions have a clear obligation to ensure that relevant employees (those who deal with customers or otherwise process the business of the institution) know that they are required to report suspicious activities to the Compliance Officer

Once an employee has reported his/her suspicion to the Compliance Officer it becomes the responsibility of the Compliance Officer, on behalf of the financial institution concerned, to make a report of the suspicious activity to the Supervisory Authority.

The Role of the Compliance Officer

4.8 The person appointed as Compliance Officer will vary according to the size of the financial institution and the nature of its business. He or she should be sufficiently senior to command the necessary authority. Larger financial institutions may choose to appoint a senior member of their compliance, internal audit or fraud departments.

4.9 The Compliance Officer should determine whether the information or other matters contained in the transaction report he or she has received give rise to a knowledge or suspicion that a customer is engaged in money laundering. In making this judgment, the officer should consider all relevant information available within the financial institution concerning the person or business to whom the initial

report relates. This may include making a review of other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship, and referral to identification records held. If after completing this review, the officer decides that there are no facts that would negate the suspicion, then he or she must disclose the information to the law enforcement agencies.

4.10 Care should be taken to guard against a report being submitted as a matter of routine to the Supervisory Authority without undertaking reasonable internal enquiries to determine that all available information has been taken into account.

4.11 The Compliance Officer will be expected to act honestly and reasonably and to make his or her determinations in good faith. Providing the officer does act in good faith in deciding not to pass on any suspicious report, there will be no liability for non-reporting if the judgment is later found to be wrong.

INTERNAL REPORTING PROCEDURES AND RECORDS

4.12 Reporting lines should be as short as possible, with the minimum number of people between the person who has developed a suspicion about a particular customer and the compliance officer. This ensures speed, confidentiality and access to the Compliance Officer.

4.13 Supervisors should also be aware of their own obligations. Supervisors should ensure that no obstacles are placed in the way of the reporting of suspicions developed by their staff to the Compliance Officer.

4.14 All suspicions reported to the Compliance Officer should be fully documented.

4.15 The Compliance Officer should acknowledge receipt of reports of suspicions from customer service staff and at the same time provide a reminder of the obligation to do nothing that might prejudice subsequent enquiries, i.e. “tipping off” which is a serious offence. All internal enquiries made in relation to the report, and the reason behind whether or not to submit the report to the authorities, should be documented.

EXTERNAL REPORTING PROCEDURES

4.15 Suspicious transaction reports under the MLPA must be lodged with the Supervisory Authority appointed pursuant to section 10 of the Act.

4.16 The Director of the ONDCP has been appointed the Supervisory Authority. His office is located at the Office of National Drugs and

Money Laundering Control Policy (ONDCP), Camp Blizard, Coolidge. Officers of the ONDCP are responsible for making a preliminary investigation into the disclosure.

Nature of the Information to be Disclosed

4.17 Sufficient information should be disclosed which indicates the nature of and reason for the suspicion. Where the financial institution has additional supporting documentation, that should be made available.

Termination of a Business Relationship Following a Disclosure

4.18 If, following a disclosure, a financial institution, exercising its commercial judgment wishes to terminate the relationship with the customer, it is recommended that before taking this step, the reporting institution should liaise with the Supervisory Authority to ensure that the termination does not "tip-off" the customer or prejudice the investigation in any way.

INVESTIGATION OF DISCLOSURES

4.19 Following receipt of a disclosure and initial research by the ONDCP, the information disclosed will usually be allocated to trained financial investigation officers in the ONDCP for a full investigation. In some circumstances it may be referred by the ONDCP to another law enforcement agency for investigation.

FEEDBACK FROM THE INVESTIGATING AUTHORITIES

Feedback on Specific Disclosures

4.20 When an enquiry is under active investigation, the investigating officer may contact the Compliance Officer to ensure that he or she has all the relevant information or to seek documentation which supports the original suspect transaction report. This may also include seeking supplementary information from the reporting institution and from other sources by way of a Court Order. The investigating officer will therefore work closely with the Compliance Officer who will receive direct feedback on the stage reached in the investigation. There may however be cases when the Compliance Officer cannot be informed of the state of the investigation, either because of the confidential nature of the enquiry, or because it is sub judice.

Section 5

5 EDUCATION AND TRAINING

STATUTORY REQUIREMENTS

5.1 Regulation 8 of the *Money Laundering (Prevention) Regulations 1999* requires financial institutions to establish a training programme designed to ensure that relevant employees within the financial institution are aware:

(i) of the institution's anti-money laundering strategy;

(ii) of the legal requirements contained in the Principal Act and the regulations.

5.2 The Regulations do not specify the nature of the training to be given, and therefore these Guidelines suggest what steps financial institutions should take to fulfil this requirement.

The Need for Staff Awareness

5.3 The effectiveness of the procedures and recommendations contained in these Guidelines must depend on the extent to which staff in financial institutions appreciate the serious nature of the background against which the Regulations have been issued. Staff must be aware of the statutory obligations of their employer to report suspicious transactions and of their own personal obligation to refrain from conduct that would amount to money laundering or aiding, abetting or being knowingly concerned in the money laundering of others. All staff should be encouraged to cooperate fully and to provide prompt reports of any suspicious transactions to their compliance officer.

5.4 It is, therefore, important that organisations conducting activities covered by the Regulations introduce manuals and training programmes to ensure that staff are fully aware of their responsibilities.

5.5 All relevant staff should be educated in the importance of the "know your customer" requirements for money laundering prevention purposes. Training in this respect should cover not only the need to know the true identity of the customer but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity at a future date. Relevant staff should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal activity.

5.6 Although Directors and Senior Managers might not be involved in the day-to-day processing of business with customers, it is important that they understand the statutory duties place on them, their staff and the institution itself. Some form of high-level general awareness raising training is therefore suggested.

TIMING AND CONTENT OF TRAINING PROGRAMMES

5.7 Timing and content of training for staff from various areas of a financial institution will need to be considered. The following is recommended:

5.8 New Employees

A general appreciation of the background to money laundering, and the subsequent need for reporting of any suspicious transactions to the Compliance Officer should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority. This training should be given at the same time as training in routine internal procedures. New staff should be made aware of the importance placed on the reporting of suspicions by the organisation and that there is a legal requirement to report.

5.9 Domestic and foreign exchange cashiers/dealers and sales persons/ advisory staff

Members of staff who are dealing directly with the public are the first point of contact with potential money launderers, and their efforts are therefore vital to the organisation's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is considered suspicious. This training should be provided at reasonably frequent intervals so that staff are kept aware of new trends in money laundering technique.

All front-line staff should be made aware of the organisation's policy for dealing with occasional customers, particularly where large cash transactions or bearer securities are involved, and of the need for extra vigilance in these cases.

Branch staff should be trained to recognise that criminal money may not only be paid in or drawn out across branch counters and should be encouraged to take note of credit and debit transactions arising from other sources, e.g. credit transfers, wire transfers and ATM transactions.

5.10 Account Opening/New Customer Personnel

Those members of staff who are in a position to deal with account opening or to accept new customers must receive the training given to cashiers, etc, in paragraph 5.9 above. In addition, the need to verify the identity of the customer

must be understood, and training should be given in the organisation's account opening and customer/client verification procedures. Such staff should be a ware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the money laundering Reporting Officer/Compliance Officer (or alternatively a line supervisory), whether or not the funds are accepted or the transactions proceeded with, and must know what procedures to follow in these circumstances.

5.11 Processing Staff

Those members of staff who process the settlement of bargains should receive appropriate training in the processing and verification procedures, and in the recognition of abnormal settlement, payment or delivery instructions. The identity of the investor and cross matching the investor's name against the cheque received in settlement is, for instance, a key process. Such staff should be made aware that the offer of suspicious funds accompanying a request to undertake investment business may need to be reported to the relevant authorities, whether or not the funds are accepted or the transaction proceeded with. Staff must know the correct procedures to follow.

5.12 Supervisors, Managers and Auditors

Training covering all aspects of money laundering control procedure should be provided to those with the responsibility for supervising or managing staff. Senior staff should be aware of the responsibilities of financial institutions under the MLPA, the regulations to the MLPA and with these guidelines. They should also be aware of trends in money laundering technique in order to be in a good position to prevent their organisation from being used for illicit purposes. Audit and compliance staff responsible for the review of procedures used by financial institutions should also be given such training in order to be in a position to deal with faults or weaknesses in systems or procedures used by the financial institutions

5.13 Compliance Officers

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

5.14 Refresher Training

It will also be necessary to make arrangements for refresher training at regular intervals to ensure that staff do not forget their responsibilities. Some financial institutions may wish to provide such training on an annual basis, others may choose a shorter or longer period or wish to take a more flexible approach to reflect individual circumstances, in conjunction with compliance monitoring.

METHOD OF PROVIDING TRAINING

5.15 There is no standard preferred way to conduct training for money laundering purposes. The training should be tailored to meet the needs of the particular financial institution, depending on the size and nature of the organisation and the available time and resources.

5.16 The Regulations do not require financial institutions to purchase specific training materials for the purpose of educating relevant staff in money laundering prevention and the recognition and reporting of suspicious transactions.

APPENDICES

APPENDIX A

EXAMPLES OF POTENTIALLY SUSPICIOUS TRANSACTIONS

Financial Institutions may wish to make additional enquiries in the following circumstances

TRANSACTIONS INVOLVING DEPOSIT TAKING INSTITUTIONS

Cash Transactions

- Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.
- Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.
- Customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.
- Company accounts whose transactions, both deposits and withdrawals, are denominated by cash rather than the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.)
- Customers who constantly pay in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments.
- Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.
- Frequent exchange of cash into other currencies without good reason.
- Branches that have a great deal more cash transactions than usual. (Head Office statistics detect aberrations in cash transactions.)
- Customers whose deposits contain counterfeit notes or forged instruments.
- Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.
- Large cash deposits using night safe facilities, thereby avoiding direct contact with deposit taking institution or financial institution staff.

Accounts

- Customers who wish to maintain a number of trustee or client accounts which do not appear consistent with the type of business, including transactions which involve nominee names.
- Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.
- Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).
- Reluctance to provide normal information when opening an account, providing minimal or fictional information or, when applying to open an account, providing information that is difficult or expensive for the financial institution to verify.
- Customers who appear to have accounts with several financial institutions within the same locality, especially when the deposit taking institution or building society is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.
- Matching of payments out with credits paid in by cash on the same or previous day.
- Paying in large third party cheques endorsed in favour of the customer.
- Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.
- Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.
- Greater use of safe deposit facilities. Increased activity by individuals. The use of sealed packets deposited and withdrawn.
- Companies' representatives avoiding contact with the branch.
- Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.
- Customers who show an apparent disregard for accounts offering more favourable terms.
- Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.

- Insufficient use of normal investment facilities, e.g. avoidance of high interest rate accounts for large balances.
- Large number of individuals making payments into the same account without an adequate explanation.
- Customers who request that account statements and other correspondence be kept at the financial institution for collection or from whom correspondence is returned “not known at this address” etc.

International banking/trading finance

- Customer introduced by an overseas branch, affiliate or other deposit taking institution based in countries where production of drugs or drug trafficking may be prevalent.
- Use of Letter 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.
- Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from: countries which are commonly associated with the production, processing or marketing of drugs; or proscribed terrorist organisations.
- Building up of large balances, not consistent with the known turnover of the customer’s business, and subsequent transfer to account(s) held overseas.
- Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account.
- Frequent requests for travellers cheques, foreign currency drafts or other negotiable instruments to be issued that are not consistent with known customer profile.
- Customers who show apparent disregard for arrangements offering more favourable terms.

Institution employees and agents

- Changes in employee characteristics, e.g. lavish life styles or avoiding taking holidays.
- Changes in employee or agent performance, e.g. the salesman selling products for cash has a remarkable or unexpected increase in performance.
- Any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

Secured and unsecured lending

- Customers who repay problem loans unexpectedly.
- Request to borrow against assets held by the financial institution or a third party, where the origin of the assets id not known or the assets are inconsistent with the customer's standing.
- Request by a customer for a financial institution to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.
- Customers who unexpectedly repay in part or full a mortgage or other loan in a way inconsistent with their earnings capacity or asset base.

Casinos and internet gaming businesses

- Customers who request that payouts be sent to third parties, particularly in jurisdictions other than their jurisdiction of domicile.
- Customers who deposit significant sums into their player accounts and then withdraw the money without having undertaken much gaming activity.
- Customers who engage in structuring.

APPENDIX B

SUMMARY OF ANTIGUA AND BARBUDA LAW ON MONEY LAUNDERING

The Antigua and Barbuda law on money laundering is contained in:— *The Money Laundering (Prevention) Act 1996; The Antigua and Barbuda Prevention of Terrorism Act 2001; The Money Laundering (Prevention) Regulations 1999.*

The Money Laundering (Prevention) Act 1996

Section 3 makes it an offence to engages directly or indirectly in a transaction that involves money or other property, knowing or having reasonable grounds for suspecting that the money or other property is derived, obtained or realised, directly or indirectly from some form of unlawful activity. It is also an offence to receive, possess, manage, invest, conceal, disguise, dispose of or bring into Antigua and Barbuda any money or other property having the same knowledge, reasonable grounds, or suspicions that the money or property is likewise from unlawful activity.

Section 5 makes it an offence to aid, abet, counsel or procure or conspire to commit money laundering.

Section 7 makes tipping off an offence, that is, where a person knows or suspects that a money laundering investigation is taking place, to divulge that fact or other information such as to prejudice the investigation.

Section 8 makes it an offence for a person to falsify conceal, destroy or otherwise dispose of or cause or permit the falsification concealment, destruction or disposal of any document or material which is or likely to be relevant to an investigation into money laundering or to any order made in accordance with the provisions of this Act.

Section 13(4) makes reporting of a suspicious transaction made in good faith by a financial institution, its employees, staff, directors, owners or other representatives as authorised by law exempted from criminal, civil and administrative liability arising from compliance with the reporting requirements of section 13(2) or any secrecy restrictions imposed by contract or law.

Section 13(5) makes it an offence for a financial institution or its employees, staff, directors, owners or other authorised representatives to wilfully fail to report suspicious financial transactions as required under section 13(2) or to wilfully make false reports. Penalty for failing to comply is $50,000.

APPENDIX C

LIST OF FINANCIAL INSTITUTIONS
(Listed in the First Schedule to the Money Laundering (Prevention) Act 1996)

1. "Banking business" and " financial business" as defined in the Banking Act and the Financial Institutions (Non-Banking) Act;
2. "International offshore Banking business" as defined in the International Business Corporation Act;
3. Venture risk capital;
4. Money transmission services;
5. Issuing and administering means of payments (e.g. credit cards, travellers' cheques and bankers' drafts);
6. Guarantees and commitments;
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 instruments (e.g., futures, options, interest rate and foreign exchange instruments etc.);
   (d) transferable or negotiable instruments;
8. Money broking;
9. Money lending and pawning;
10. Money exchange (e.g., *casa de cambio*);
11. Real property business;
12. Credit unions;
13. Building societies;
14. Trust business.
15. Casinos
16. Internet gambling
17. Sports betting
18. Insurance Business
19. Dealers in jewellery, precious metals or art