

THE COMPLIANCE COMMISSION OF THE BAHAMAS

ANTI-MONEY LAUNDERING
&
ANTI-TERRORISM FINANCING

HANDBOOK & CODE OF PRACTICE

FOR

FINANCIAL AND CORPORATE
SERVICE PROVIDERS

(Excluding financial and corporate service providers that only offer corporate registry services)

THE COMPLIANCE COMMISSION

Second Floor Charlotte House
Charlotte Street
P. O. Box N-3017
Nassau, BAHAMAS

Tel: (242) 397-4198

Fax: (242) 322-6968

E-mail: compliance@bahamas.gov.bs

Web address: www.bahamas.gov.bs/compliance

Revised - July 2009

© All rights reserved - The Compliance Commission of The Bahamas

EXPLANATORY FOREWORD

The Inspector of Financial and Corporate Services “the Inspector” has power under section 11(3)(b) of the Financial and Corporate Service Providers Act (FCSPA) to ensure that its licensees comply with the requirements for anti-money laundering (AML) and combating the financing of terrorism (CFT) found in the AML laws. The Inspector and the Compliance Commission “the Commission” pursuant to the framework for supervisory cooperation between Bahamian regulators contained in their respective governing statutes have agreed that the Commission would have responsibility for the AML supervision of FCSPs, including the conduct of the AML examination process. For this purpose the Commission has issued this Code of Practice (Code) for licensed financial and corporate service providers (FCSPs). Copies of all Codes of Practice issued by the Commission are available electronically on its website.

Obligations imposed by this Code are enforceable in accordance with both the FCSPA and the Financial Intelligence (Transactions Reporting) (Amendment) Regulations 2009 (FITRR).

All references in this document to AML include obligations for CFT under the Anti-Terrorism Act, Chapter 107 unless the context requires otherwise.

FCSPs are identified as financial institutions subject to AML regulation by virtue of section 3(1)(m) of the FTRA.

This Code has been issued for persons or companies holding FCSPs licences and which provide financial intermediary services involving the handling of funds on behalf of third parties. **N.B. - Those FCSPs that only offer corporate registry, corporate directors, officers and nominee shareholders do not fall within the scope of this Code.**

This Code is intended to provide FCSPs with practical guidance and examples of good practice on how to implement the requirements of the AML legislation. It also supports the regulatory objective of maintaining the reputation of The Bahamas as a first-rate international business centre with zero tolerance for criminal activity. This Code updates the first Code published for FCSPs in 2002 and its revisions since that date.

Unless the context requires otherwise, the masculine terminology used throughout the document includes the feminine gender and the singular terminology includes the plural.

The Commission intends to issue periodic directions to supplement this Code as changing circumstances dictate.

Finally, the Commission would like to express its gratitude to all those in the profession, representative bodies and Regulators that contributed to the development of this Handbook and Code.

MR. PHILIP B. STUBBS
CHAIRMAN
THE COMPLIANCE COMMISSION &
THE INSPECTOR OF FINANCIAL AND CORPORATE SERVICES
30th July, 2009

INDEX

PART		PAGE
A	DEFINITIONS	3
B	BACKGROUND	6
	I MONEY LAUNDERING AND TERRORISM FINANCING	7
	1 Money Laundering	7
	2 Terrorism Financing	7
	3 The Global Fight against Money Laundering	8
	II THE LEGISLATIVE AND REGULATORY STRUCTURE FOR AML/CFT IN THE BAHAMAS	10
	4 The Legislative Framework	10
	5 The Regulatory Framework	10
	III THE FCSP AS A FINANCIAL INSTITUTION	12
	6 When is a FCSP a financial institution?	12
	IV SUPERVISORY FRAMEWORK OF THE COMMISSION	13
	7 The Commission	13
	8 The Examination Process	15
	▪ On-site	15
	▪ Off-site	15
	▪ Types of Examination	16
	○ Routine	16
	○ Follow-up	18
	○ Random	19
	○ Special	19
	9 Examinations for Financial and Corporate Service Providers under section 11 (3) (b) of the Financial and Corporate Service Providers Act	20
	10 Commission awareness and training programmes for FCSPs	21
C	INTERNAL AML/CFT PROCEDURES	22
	V PERIODIC INTERNAL REVIEW OF AML/CFT SYSTEMS	23
	11 Internal testing of compliance levels	23
	VI CLIENT IDENTIFICATION/VERIFICATION (KYC) PROCEDURES	24
	12 Guidance on risk-based KYC procedures	24
	▪ Low risk characteristics	25
	▪ Due diligence for low risk customers/clients	26
	▪ High risk characteristics	28
	▪ Enhanced due diligence for high risk customers/clients	29
	13 Verification details and documentary evidence procedures	31
	▪ When must verification take place?	31
	▪ Individuals	33
	▪ Corporate bodies	33
	▪ Partnerships and unincorporated associations	35
	▪ Verification of facilities/accounts for intermediaries	36
	▪ Additional guidance on verification in the case of trusts	36
	▪ Verification when providing safe custody and safety deposit boxes	37
	▪ Verification of unverified pre-2001 facilities	37
	▪ Guidance on confirming the identity of a client	38
	▪ Guidance on verifying address	38

PART		PAGE
	14 Third Party (or Eligible) introductions from another financial institution	39
	15 Monitoring of Facilities	42
VII	RECORD KEEPING PROCEDURES	43
	16 Statutory requirements to maintain records	43
	▪ Format of records	43
	▪ Identification/verification (KYC) records	43
	▪ Transaction records	44
	▪ When records need not be kept	45
	○ Special considerations for record keeping retention on the liquidation of a financial institution.	45
	▪ Destruction of Records	45
VIII	PROCEDURES FOR THE RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS	46
	17 The Financial Intelligence Unit (the FIU)	46
	▪ The mandatory requirement to appoint a Money Laundering Reporting Officer (MLRO)	46
	▪ The role of the MLRO	46
	▪ The mandatory requirement to appoint a Compliance Officer	47
	▪ Recognition of suspicious transactions	47
	▪ Internal reporting of suspicious transactions	48
	▪ Procedure for reporting suspicious transactions	49
	▪ Feedback from the FIU	50
XI	STAFF RECRUITMENT, EDUCATION AND TRAINING PROCEDURES	51
	18 Know Your Employee (KYE) Procedures	51
	19 Staff Awareness Programmes	51
	20 Staff Education and Training Programmes	52
	▪ New employees	52
	▪ Frontline staff that deal directly with the public for the purpose of receiving and making payments, deposits etc. such as cashiers/ accounts officers	52
	▪ Administration/operations supervisors and managers	52
	▪ MLROs/Compliance Officers	53

APPENDICES

		Page
A	Summary of Bahamian Law on AML/CFT	54
B	First Schedule FTRA Countries & Approved Stock Exchanges	55
C	Examination Form for FCSPs	56-67
D	Commission's Evaluation Process	68
E	Matrices of Money Laundering Offences under POCA, FTRA, FI(TR)R and ATA	69-72
F	Enquiry form for confirmation of identity	73
G	Sample STR to FIU	74-78
H	FCSPs Typology Examples	79
FIGURES:		
	1. <i>Regulatory Structure for AML in The Bahamas</i>	11
	2. <i>Graphic illustration of a FCSPs' obligations under the AML laws</i>	12
	3. <i>What is structuring?</i>	32

A. DEFINITIONS

“**AML**” means anti-money laundering

“**AML laws**” means the Proceeds of Crime Act, the Financial Transactions Reporting Act, the Financial Intelligence Unit Act, the Anti-Terrorism Act and all Regulations, Guidelines, Codes and other subordinate instruments made under these Acts. For a complete list of the legislation and citations see **Appendix A**

“**ATA**” means the Anti-Terrorism Act, Ch. 107

“**BICA**” means The Bahamas Institute of Chartered Accountants

“**cash**” means, coins, paper money, travelers’ cheques, postal money orders and other similar bearer-type negotiable instruments

“**CFATF**” means the Caribbean Financial Action Task Force

“**CFT**” means combating the financing of terrorism

“**CO**” means Compliance Officer

“**Commission**” means the Compliance Commission established under section 39 of the FTRA

“**constituents**” means the financial institutions identified in section 46 of the FTRA for which the Commission has AML supervisory responsibility

“**customer due diligence**” or “**CDD**” - The objective of customer due diligence which is sometimes referred to as KYC, is to ensure that reasonable steps are taken to satisfy the firm that the client is who he claims to be and that his funds are derived from a legitimate source or are not intended to be used for terrorism

“**DNFBP**” means a designated non-financial business and professional in accordance with Recommendation 12 of the FATF 40+9 Recommendations

“**eligible introducer**” means -

- (1) any other Bahamian financial institution under section 3 of the FTRA ; or
- (2) any foreign financial institution from a country in **Appendix B** that is:
 - a licensed bank;
 - a licensed trust company;
 - a licensed casino;
 - a person regulated by the equivalent of the Securities Commission of The Bahamas;
 - any life insurance company regulated by the equivalent of the Office of the Insurance Commission; and
 - any person licensed and regulated by the equivalent of the Inspector of Financial and Corporate Services.

“FATF” means the Financial Action Task Force

“facility” is any account or arrangement that is provided by a FCSP to a client by, through or with which the client may conduct two or more transactions whether or not they are so used. A facility in the case of a FCSP is essentially any of those services that would qualify him to be a financial institution as set out in the preceding paragraph. It also specifically includes provision of facilities for safe custody, such as safety deposit boxes

“facility holder” is the client and any person who is authorized to issue instructions in relation to how transactions should be conducted through a facility provided by the FCSP

“FCSP” means a financial and corporate service provider licensed under the Financial and Corporate Service Providers Act

“financial institution” means a person or entity described in section 3 of the FTRA who or which provides financial intermediary services and on who have been imposed AML obligations pursuant to the AML laws

“Financial Intermediary Services” are those services where the FCSP facilitates the movement of funds into, out of and around the financial system and includes being a signatory on the client’s bank account irrespective of the location of the account or the location of the other signatories to the account

“FI(TR)R” means the Financial Intelligence (Transactions Reporting) Regulations, Ch. 367

“FIU” means the Financial Intelligence Unit

“FIUA” means the Financial Intelligence Unit Act, Ch. 367

“FTRA” means the Financial Transactions Reporting Act, Ch. 368

“FTRR” means the Financial Transactions Reporting Regulations, Ch. 368

“know your client/customer” or “KYC” which is also referred to as customer due diligence, is designed to ensure that reasonable steps are taken to satisfy the firm that the client is who he claims to be and that his funds are derived from a legitimate source or are not intended to be used for terrorism

“MLRO” means money laundering reporting officer

“occasional transaction” means any one-off transaction including, but not limited to cash, that is carried out by a person otherwise than through a facility in respect of which that person is a facility holder. An example of this may be where someone purports to pay a sum in cash over \$15,000 to the firm for the benefit of a facility holder of that firm

“para.” means paragraph

“POCA” means the Proceed of Crime Act, Ch. 93

“politically exposed persons” or “PEPs” is the term used to describe natural persons who are or have been entrusted with prominent public functions, their immediate family members and persons known to be close associates of such persons. It includes:

- (a) Heads of State, Heads of Government, Ministers and Deputy or Assistant Ministers;
- (b) Members of Parliament;

- (c) Members of Supreme Courts, Constitutional Courts or other high-level judicial bodies;
- (d) Members of Boards of Central Banks;
- (e) Ambassadors, Charges d'affaires and high-ranking officers in the armed forces or law enforcement;
- (f) Members of the Administrative, Management or Supervisory Boards of State-owned enterprises;
- (g) Immediate family members of any of the above such as:
 - a spouse,
 - a partner (including a person who is considered by his national law as equivalent to a spouse),
 - children and their spouses, and
 - parents;
- (h) Persons known to be close associates of persons identified in (a) through (f) above, such as:
 - any person who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any close business relations, with a PEP, and
 - any individual who has sole beneficial ownership of a legal entity or legal arrangement which has been established for the benefit of a PEP.

“STR” means a suspicious transaction report

“transaction” means any deposit, withdrawal, exchange or transfer of funds in cash, by cheque, payment order or other instrument, and includes electronic transmissions of funds

B. BACKGROUND

This part describes the phenomenon of money laundering and terrorist financing, provides background and general introductory information on the money laundering and terrorist financing regulatory framework of The Bahamas and the global efforts against money laundering and terrorist financing.

It also covers the details of the supervisory framework of the Commission. This supervisory framework includes an on-site and off-site examination process for financial and corporate service providers and an AML/CFT education and training programme for FCSPs.

I. MONEY LAUNDERING AND TERRORISM FINANCING

1 MONEY LAUNDERING

- 1.1 Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. Its purpose is to allow them to maintain control over those proceeds and ultimately provide a legitimate cover for the source of their income.
- 1.2 There is no one single method of laundering money. Methods range from the purchase and resale of real property and luxury items (e.g., cars or jewelry) to passing money through a complex international web of legitimate businesses and “shell” companies. Initially, however, in the case of drug trafficking and some other serious crimes, the proceeds usually take the form of cash which needs to enter the financial system by some means.
- 1.3 Despite the variety of methods employed, the laundering process is accomplished in three stages, which may comprise numerous transactions, and which could alert a financial institution to criminal activity: These stages are:
- (1) **placement**, which is the physical disposal of cash proceeds derived from illegal activity;
 - (2) **layering**, which involves the separation of illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity; and
 - (3) **integration**, which is 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.
- 1.4 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 depend on the available laundering mechanisms and the requirements of the criminal or his organization.

2. TERRORISM FINANCING

- 2.1 Unlike money laundering, which focuses on the origin of the funds in question, terrorism financing looks at the destination of the funds which may in fact originate from a legitimate source.
- 2.2 Terrorism financing is the method by which “directly or indirectly, unlawfully and willfully, persons provide or collect funds with the intention that the funds should be used or in the knowledge that the funds are to be used, in full or in part in order to carry out (a) an act which constitutes an offence within the scope of and as defined in one of the treaties listed in the First Schedule to the ATA¹; or (b) any other act intended to cause death or serious bodily injuries to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an

¹ See Appendix A.

international organization to do or to refrain from doing any act.”²

- 2.3 The United Nations (UN) under UNSCR 1373 has produced a list of designate persons/ countries with known or suspected terrorist connections. This list is updated periodically and is forwarded onto the UN’s contact in each jurisdiction. In the case of The Bahamas, this is the Ministry of Foreign Affairs.

3 THE GLOBAL FIGHT AGAINST MONEY LAUNDERING

3.1 The Financial Action Task Force (FATF)

- 3.1.1 The FATF was founded by the Governments of the G7 leading industrialized nations in 1989. The FATF is the main international body for tackling money laundering and terrorist financing. The FATF is an inter-governmental body which develops and promotes policies, both nationally and internationally, to combat money laundering. Further information on the FATF can be found at www.fatf-gafi.org.

- 3.1.2 The FATF has developed forty (40) Recommendations on tackling money laundering and nine (9) Special Recommendations on combating terrorism financing. The 40 + 9 Recommendations set out the framework for AML and CFT initiatives and are designed for universal application. They provide a complete set of counter-measures against money laundering and terrorist financing covering the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation.

- 3.1.3 Recommendation 12 of the FATF’s 40+9 Recommendations calls on countries to establish an AML supervisory framework to regulate designated non-financial businesses and professionals (DNFBPs).

- 3.1.4 Under Bahamian law the implementation of Recommendation 12 (d) and (e) occurs through section 3 (1) (h) and (j) through (m) of the FTRA.

- 3.1.5 The FATF has also promoted the concept of regional organizations along the lines of its own structure, whose goals would be to raise awareness of money laundering and terrorist financing and introduce regional evaluation programmes to monitor the implementation of the 40 + 9 Recommendations, amongst other things.

3.2 The Caribbean Financial Action Task Force (CFATF)

- 3.2.1 The CFATF was established as part of the efforts of the FATF to establish regional style bodies patterned after the FATF. The CFATF came into existence as a result of three regional meetings of Governments in 1990, 1992 and 1993.

- 3.2.2 At the 1992 meeting the Kingston Declaration called for the establishment of a Regional Secretariat. The Secretariat was established during early 1994, in Trinidad and Tobago, and funded by the FATF donor countries. The Chair of CFATF is rotated annually amongst its members. Further information on the CFATF and its work can be viewed on its website at www.cfatf@cfatf.org.

- 3.2.3 The Bahamas is one of the founding members of CFATF. The Bahamas’ AML regime is evaluated every four years by CFATF.

² UN 1999 International Convention for the Suppression of the Financing of Terrorism.

3.3 Financial Sector assessments by the International Monetary Fund (IMF)

- 3.3.1 The Bahamas, as a member of the IMF, also participates in the IMF's financial sector assessment programme (FSAP). The FSAP, a joint IMF and World Bank effort introduced in May 1999, aims to increase the effectiveness of efforts to promote the soundness of financial systems in member countries. Supported by experts from a range of national agencies and standard-setting bodies, work under the program seeks to identify the strengths and vulnerabilities of a country's financial system; to determine how key sources of risk are being managed; to ascertain the sector's developmental and technical assistance needs; and to help prioritize policy responses. Detailed assessments of observance of relevant financial sector standards and codes (including the FATF's 40+9 Recommendations), which give rise to Reports on Observance of Standards and Codes (ROSCs) as a by-product, are a key component of the FSAP. These generally occur on a five-year cycle.

II. THE LEGISLATIVE AND REGULATORY STRUCTURE FOR AML/CFT IN THE BAHAMAS

4 THE LEGISLATIVE FRAMEWORK

4.1 The Bahamian substantive law relating to AML is contained in:

- the Proceeds of Crime Act
- the Financial Transactions Reporting Act
- the Financial Transactions Reporting Regulations
- the Financial Intelligence Unit Act
- the Financial Intelligence (Transactions Reporting) Regulations, and
- the Anti-Terrorism Act

4.2 A summary overview of the laws can be found in **Appendix A**. These laws, as well as others referred to in this Handbook can be viewed in full and downloaded from <http://laws.bahamas.gov.bs>.

4.3 The legislation, which includes all subsequent amendments and subordinate legislative measures sets out procedures which are designed to achieve two purposes: firstly, to enable suspicious transactions to be recognized as such and reported to the authorities; and secondly, to ensure that if a customer comes under investigation in the future, a financial institution can provide its part of the audit trail.

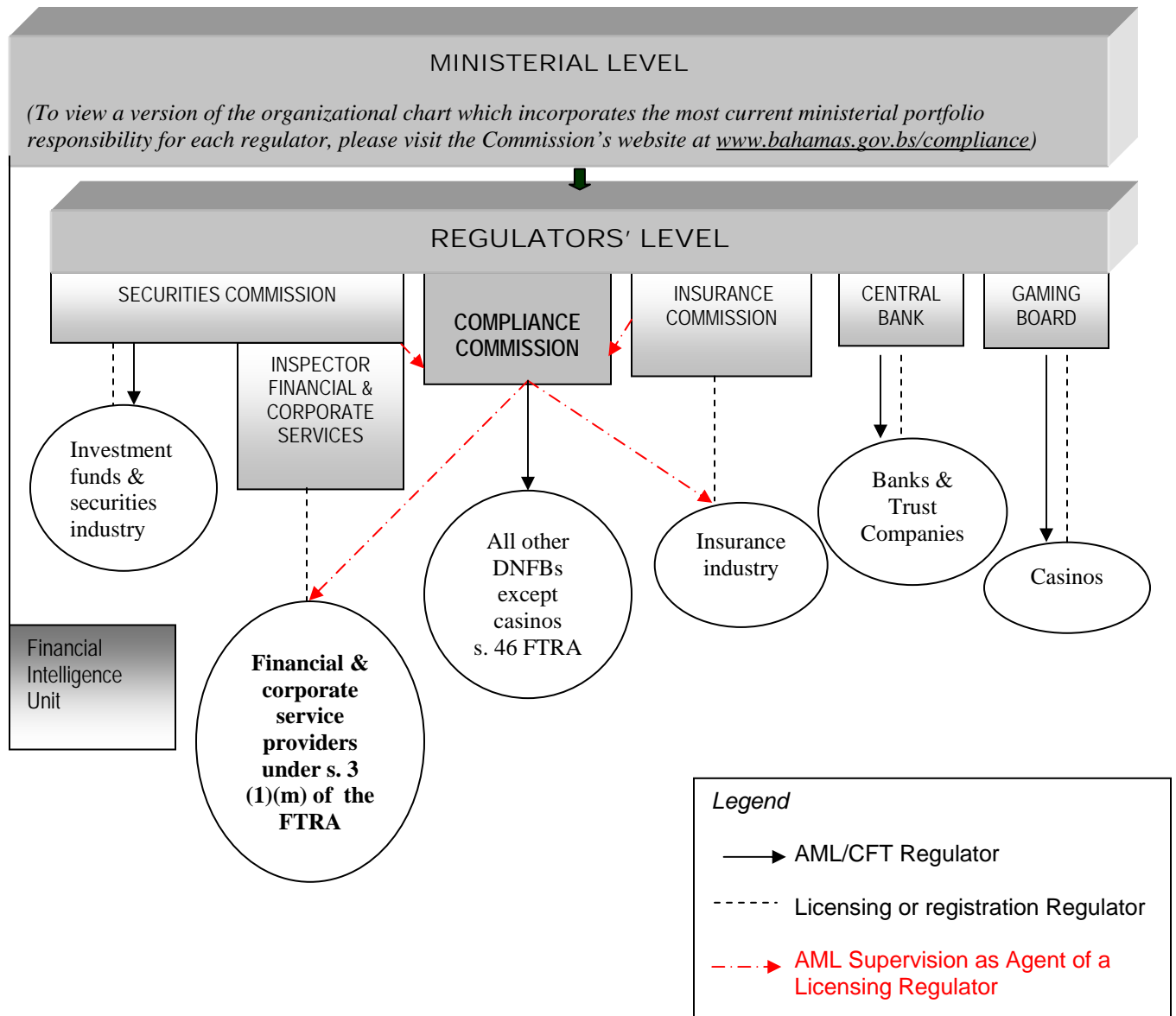
5. THE REGULATORY FRAMEWORK

5.1 An organizational chart of the AML regulatory framework, specifically identifying FCSPs, is found in **Fig. 1** below. The Central Bank regulates the banking and trust companies industry, the Securities Commission regulates the securities and investment funds industry, the Insurance Commission regulates the insurance industry, the Inspector of Financial and Corporate Services regulates financial and corporate service providers and the Gaming Board regulates casinos. The authority for the Commission to supervise the financial institutions within its remit is found in section 46 of the FTRA.

5.2 The Financial Intelligence Unit or FIU is the agency charged, amongst other things, with receiving and analyzing suspicious transactions reports from financial institutions (See paras. **17.1** to **17.4** for more details about the FIU).

5.3 It will be noted from the organizational chart that the Commission supervises both the FCSPs and the insurance industry for AML purposes under the authority of an arrangement for regulatory cooperation, respectively with the Inspector of Financial and Corporate Service and the Insurance Commission. The Commission also administers the AML on-site examination for these sectors. All other regulatory requirements, apart from AML supervision for these sectors (i.e. licensed FCSPs and insurers) are administered by the Regulator responsible for licensing and/or registration of the business activities of the licensee.

Figure 1: Regulatory Structure for AML in The Bahamas



III. THE FINANCIAL AND CORPORATE SERVICE PROVIDER AS A FINANCIAL INSTITUTION

6. WHEN IS A FCSP A FINANCIAL INSTITUTION?

6.1 FCSPs in The Bahamas are subject to the anti-money laundering laws where services rendered by them involve facilitating the entry or placement, movement, or removal of funds into, within or out of the financial system on behalf of clients in circumstances where the FCSP merely acts in relation to those funds, as an agent, intermediary or conduit for the client.

Fig. 2: Graphic Illustration of FCSPs' Obligations under the AML Laws.

FCSP

Service Provided	Financial Transaction Services: Section 3 (1) (m) of the FTRA Services involve the licensee in facilitating the entry or placement, movement, or removal of funds, into, within or out of the financial system.	Corporate Services: Section 2 of the FCSPA Corporate Registry services including nominee directors, shareholders, incorporations, corporate filings etc. which do not involve the licensee in any movement of funds on behalf of the client.
Supervisory Authority	The Commission, under the authority of an arrangement for regulatory cooperation with the Inspector of FCSP supervises FCSPs for AML purposes in relation to these services.	The Inspector of FCSPs is responsible for supervising these services.
Legislative Obligations	Activities subject to the AML laws and guidelines of the FTRA, FTRR, FI(TR)R, and this Code.	Activities subject to obligations under the FCSPA.
	ALL services provided by a FCSP are subject to the general AML requirements under the Proceeds of Crime Act Ch 93	

IV. SUPERVISORY FRAMEWORK OF THE COMMISSION

7. THE COMMISSION

7.1 The establishment of the Commission

7.1.1 Section 39 of the FTRA establishes the Commission as a body corporate for the purpose of ensuring that financial institutions within its constituency (as set out in section 46 of the FTRA) comply with the provisions of the FTRA. The Commission consists of three members appointed by the Governor-General.

7.1.2 The Commission has the same functions and powers of the Inspector with respect to AML supervision.

7.2 Functions and powers of the Commission

7.2.1 The Commission has a two-fold function, namely:-

- to maintain a general review of financial institutions for which it has supervisory responsibility, in relation to the conduct of financial transactions and to ensure compliance with the provisions of the FTRA, the FI(TR)R and guidelines issued by the FIU; and
- whenever the Commission deems such to be necessary to conduct on-site examinations of its constituent financial institutions for the purpose of ensuring compliance with the provisions of the AML laws and regulations. The Commission can appoint an auditor, at the expense of the FCSP firm, who will conduct such examination and report thereon to the Commission.

7.2.2 The Commission is empowered to:

- do all things necessary for the performance of its functions including entering into contracts;
- require production of records and the supply of information/explanation;
- require, at all reasonable times, a financial institution to produce transaction records, verification records and any other records prescribed by Regulations that must be kept under the FTRA;
- require financial institutions to provide such information or explanation, as it may reasonably require, for the purpose of enabling the Commission to perform its functions under the FTRA; and
- periodically issue Codes of Practice, particularly to provide guidance as to the duties, requirements and standards to be complied with and the procedures (whether as to verification, record-keeping, reporting of suspicious transactions or otherwise) and best practices to be observed by its constituent financial institutions in meeting their obligations under the FTRA and other AML laws.

7.2.3 The Commission supervise FCSPs for AML purposes under the authority of an arrangement for regulatory cooperation with the Inspector of Financial and Corporate Services.

7.3 How does the Commission supervise FCSPs for AML purposes?

7.3.1 The Commission supervises FCSPs, through a combination of on-site and off-site examinations, and education, training and awareness programmes. In addition, periodic directions, intended to supplement the Codes of Practice are issued.

7.3.2 The Commission also has established a programme of engagement annually with the representative bodies of the financial institutions that it regulates. Separate consultative meetings are held each January with the Inspector of Financial and Corporate Services, amongst other bodies, to review the activities of the previous year and to discuss plans for the ensuing year.

8. THE EXAMINATION PROCESS

8.1 The Commission carries out its AML supervision of FCSPs by means of on-site and off-site examination programmes.

8.2 Within this framework, there are four types of examination which the Commission administers:

- routine (which may be either an on-site or an off-site examination),
- follow-up (on-site only),
- random (on-site only), and
- special (on-site only).

8.3 The most important of these four examinations is the routine examination as it provides a periodic assessment that tests both the adequacy and currency of measures and programmes implemented by a FCSP to satisfy its AML obligations. Further details on the procedures for the examination types can be found at para. **8.6** below.

8.4 On-Site Examinations

8.4.1 Under section 43 (b) of the FTRA, the Commission is mandated to conduct on-site examinations.

8.4.2 **N.B.: The on-site examination is not an audit of the business activities. It is simply the process by which the Commission ensures that the AML laws are being fully complied with.**

8.4.3 With the exception of the routine examination which must be conducted by a licensed public accountant, duly appointed by the Commission and the Inspector, all other types of on-site examinations are conducted by the Commission's Inspection Unit.

8.5 Off-Site Examinations

8.5.1 In order to conduct an off-site examination, the FCSP must first obtain from the Commission, a waiver from the routine on-site examination.

Waiver from the routine on-site examination

8.5.2-1 A waiver exempts a FCSP from the requirement to submit to a routine on-site examination during a given examination year. A waiver is granted based on all of the following criteria being met:

- the financial institution must have submitted to at least one (1) on-site examination;
- previous examination(s) should reveal that the institution has complied with AML laws including relevant Policies and Procedures;
- the critical areas of the examination e.g. customer verification, suspicious transaction reporting, etc. reveal no deficiencies; and
- the institution has not increased its total facility count by more than twenty-five percent (25%) within one year of its last examination.

- 8.5.2-2 Where a waiver has been granted a FCSP will instead be required to conduct an off-site examination during such period.
- 8.5.2-3 For the off-site examination, the FCSP is required to have a Senior Officer (preferably the Money Laundering Reporting Officer) complete the examination form in-house and forward it onto the Commission's office. This completed examination form will be evaluated by the Commission's staff in the same manner as a return for an on-site examination. The Commission, in turn, will communicate any concerns arising from the assessment to the FCSP. (See para. **8.6.2-2** for the *Follow-up Examination* process).
- 8.5.2-4 The completed examination form must be submitted to the Commission by the 31st January immediately following the period covered by the examination.

N.B. During the period of a waiver, the financial institution is not precluded from selection for a random examination (see para. 8.6.3), or for a special examination (see para. 8.6.4), both of which are conducted by the Commission's Inspection Unit.

8.6 Types of examination

8.6.1 Routine Examination

- 8.6.1-1 The routine examination may take the form of either an on-site examination or an off-site examination. The examination form found in **Appendix C** is used to evaluate the FCSP's compliance levels.

- 8.6.1-2 **N.B. The routine examination takes the form of an "agreed upon procedure" designed to test the adequacy of AML systems that have been implemented by a FCSP for the purpose of meeting its obligations under the AML laws and regulations. The "agreed upon procedure" was developed in conjunction with BICA.**

- 8.6.1-2 The Commission determines, on a risk-sensitive basis, when a supervised financial institution should be required to undergo an on-site examination, having due regard for the adequacy of its policies and procedures for AML and CFT and the application of the guidance contained in this document.

- 8.6.1-3 A FCSP which has developed and enforces sound AML policies and procedures, poses less risk for money laundering and terrorist financing than a financial institution which has no or less stringent policies and procedures. Consequently, the higher the money laundering/terrorist financing risk, the more vigorous supervision will be applied.

- 8.6.1-4 Effective 1st January, 2009, the Commission's examination year for the routine examination runs from **1st January to 31st December of each year**. For each annual period, all FCSPs that provide financial intermediary services must submit those aspects of their business to a routine examination. This routine examination must be an on-site examination unless the FCSP has been granted a waiver from the Commission exempting it from the on-site examination for that year. (See para. **8.5.2** above for information on waivers). For any period during which a supervised FCSP has been granted a waiver from the on-site examination, it must instead ensure that an off-site examination is carried out. The examination, (whether on-site or off-site), must be completed during the month of January immediately following the period covered by the examination.

- 8.6.1-5 A routine on-site examination must be conducted by a licensed public accountant, that has been duly appointed by the Commission and the Inspector.

The examining licensed public accountant must obtain a Letter of Appointment³ from the Commission before he commences the examination. Letters of Appointment are issued for the duration of a licensed public accountant's current BICA licence.

8.6.1-6 A FCSP may select the licensed public accountant of its choice, however the examining accountant must be independent of the FCSP and the FCSP should satisfy itself that the examiner has a current and valid letter of appointment.

8.6.1-7 A routine examination assesses the FCSP's compliance with the AML laws i.e. the FTRA, FTRR, the FI(TR)R, this Code and the FIU Guidelines. The examination (see examination form at **Appendix C**) reviews the procedures/practices in place for the five (5) operational areas of the FCSPs' financial intermediary activities as follows:

- (1) the verification/identification of customers;
- (2) maintenance of customer verification and transaction records;
- (3) reporting of suspicious transactions to the FIU;
- (4) assignment of a MLRO; and
- (5) the internal procedures for training personnel on money laundering detection and prevention as required by the FI(TR)R.

8.6.1-8 In the case of a routine on-site examination, once completed, the examining accountant should discuss the contents of the examination form with the financial institution. Within 10 days of completing the examination form the examining accountant must submit the completed examination form to the Commission to be evaluated. Please see **Appendix D** for an overview of the Commission's evaluation process. Those FCSPs that receive an adverse rating on the routine on-site examination will be scheduled for a follow-up examination.

8.6.1-9 Frequency of the routine on-site examination

8.6.1-9(a) With effect from 1st January 2009, upon the written application of a FCSP, the Commission will issue written directions to a FCSP regarding the next date for a routine on-site examination taking into account the following considerations:

- an evaluation of the FCSP's risk-based policies and procedures for combating money laundering and terrorist financing to determine their adequacy;
- whether the FCSP has met all of its examination requirements, dating back to the effective date of the FTRA, i.e. 1st January, 2001; and
- an evaluation by the Commission of all previous examinations completed in relation to the FCSP to determine the FCSP's level of compliance with its statutory obligations under the AML laws and the Commission's Codes of Practice.

³ A Letter of Appointment is a document issued to licensed accountants by the Commission, the Inspector and the Registrar of Insurance authorizing them to conduct on-site examinations as its agents. This document indemnifies the accountant from any action which may arise in the course of or as a result of the examination.

8.6.1-9(b) TRANSITIONAL ARRANGEMENTS FOR THE PERIOD 1ST AUGUST 2008 TO 31ST DECEMBER 2009

The Commission's examination year is based on the calendar year (1st January to 31st December). Prior to the change to the calendar year, financial institutions were required to submit examinations for the period 1st August to 31st July of the following year.

Those financial institutions which did not submit to an examination for the period 1st August, 2007 to the 31st July 2008 (excluding those exempted by the Commission for that period) were expected to submit all outstanding examinations on or before 30th January, 2009.

All financial institutions are now required to submit examinations returns by the 31st January each year for off-site or on-site examinations.

8.6.2 Follow-up Examination

8.6.2-1 Follow-up examinations are always on-site examinations and are solely for the purpose of addressing the deficiencies of the AML systems of FCSPs that are revealed through the routine or off-site examination process. Such examinations are specific in scope and will focus on identified weaknesses. Follow-up examinations are conducted by the Commission's Inspection Unit.

8.6.2-2 Procedure for follow-up visits

8.6.2-2(a) Where an adverse rating is given a Notice is issued advising of a follow-up examination to take place within five (5) working days of the Commission completing the evaluation on a return. Unless otherwise stated, financial institutions are given up to three (3) months to rectify all deficiencies discussed during the follow-up visit.

8.6.2-2(b) Below are the steps for Follow-up Examinations.

Step 1. The Commission contacts the financial institution to arrange a meeting with the Management and/or the MLRO two (2) weeks prior to the meeting date. The purpose of the meeting is to discuss the results of the routine examination.

Step 2. During the meeting, the inadequacies of the AML systems are clearly identified and a strategy is devised for addressing them.

Step 3. A date is set within one (1) month for the Commission to revisit the financial institution to determine the level of progress.

8.6.2-2(c) Where sufficient progress is evident, no further visit is made regarding those issues and a report to this effect is made.

8.6.2-2(d) However, if a financial institution does not adhere to the strategy outlined for resolving the inadequacies of their AML system, the following steps below are taken.

Step1. A letter is forwarded to the financial institution highlighting the details of previous meetings including minutes from any prior

meeting reminding it of the agreed-upon strategy for addressing inadequacies of the entity. A period of two (2) weeks is given for the financial institution to rectify all inadequate systems.

Step 2. The examiner visits the financial institution at the end of the two (2) week period to determine whether the problems have been remedied.

Step 3 Where the systems are examined and seem adequate, a final report is written to this effect. If there is insufficient progress, a report is written and forwarded to the Commissioners who will determine whether legal action is to be pursued.

8.6.2-2 (e) In case of a financial institution that is regulated by another financial services Regulator, copies of all communication, reports recommendations etc. are forwarded to the relevant regulator.

8.6.3 *Random Examination*

8.6.3-1 In addition to the routine examination, FCSPs are also subject to random on-site examinations by the Inspection Unit of the Commission. The primary purpose of the random examination is to test the routine examination process.

8.6.3-2 The assessment process to be followed for a random examination is the same as that for the routine examination process (see para. **8.6.1**).

8.6.3-3 In the case of a random examination, a notice will be sent to the financial institution at least two weeks prior to the examination. This notice will be forwarded to the MLRO or the Senior Management of the FCSP.

8.6.4 *Special Examination*

8.6.4-1 The Commission will conduct an on-site examination of a FCSP in “special” circumstances, based on cause, to determine whether there has been any infraction of the AML laws and the extent of the violation. Such an examination will usually take place where a financial institution has violated any provision of the AML laws, or where information comes to the attention of the Commission that a statutorily prescribed financial institution is providing financial services despite having advised the Commission to the contrary.

8.6.4-2 Depending on the nature of the circumstances which give rise to invoking this approach, the procedure may be either a full examination as in the case of a routine examination, or an investigation directed towards a specific issue.

9 EXAMINATION FOR FINANCIAL AND CORPORATE SERVICE PROVIDERS UNDER SECTION 11(3)(b) OF THE FCSPA

9.1 A holder of a FCSP licence is also subject to an examination of its corporate services under section 11 (3) (b) of the FCSPA in addition to the AML on-site examinations set out in paragraphs 8.6.1-8.6.4.

9.2 To minimise disruption to FCSPs, the Commission and the Inspector of FCSPs have agreed the **the examination form (Appendix C) would consist of two parts, sometimes referred to as the “Combined Form”**. **The first part deals with the obligations in respect of corporate services, whilst the second deals with obligations which the licensee has under the AML laws by virtue of providing financial intermediary services. Where an FCSP does not provide services to its clients that involves facilitating the movement of funds into, around or out of the financial system, only the first part of the form needs to be completed.**

9.3 On completion of an examination the first part of the examination form is detached and forwarded to the Inspector. The second part of the examination form remains with the Commission and is dealt with in accordance with the procedures set out in section 8 above.

10. COMMISSION AWARENESS AND TRAINING PROGRAMMES FOR FCSPs

- 10.1 The Commission in conjunction with the Inspector of FCSPs organises annual training programmes for FCSPs. In addition, officers of the Commission are available for specific training programmes for individual FCSPs upon request.
- 10.2 As a tool of supervision, the Commission also convenes a meeting at the beginning of each year with the Inspector of FCSPs. The purpose of these meetings is to collaborate and to discuss any AML concerns of the FCSP industry and the Commission.

C. INTERNAL AML/CFT PROCEDURES

This part provides some guidance on implementing the internal AML procedures to give effect to the obligations in:

- Parts II, III, and IV of the FTRA and the FTRR that deal respectively with customer verification/identification (sections **12-14**), record-keeping (section **16**) suspicious transactions and reporting (section **17**);
- Regulation 5 of the FITRR which call for the implementation of internal procedures for identification, record keeping, suspicious transaction reporting and staff awareness, education and training⁴ (sections **12-20**).

The Commission supports and encourages FCSPs to implement a risk-based framework for addressing AML vulnerabilities posed to the entire firm. The process of implementing such a framework involves putting in place procedures for identifying the money laundering and terrorist financing risks facing the FCSP, given its clientele, products and services. FCSPs should have regard to all available information, including published money laundering typologies⁵ or terrorist lists, to assist with identifying potential risks.

In order for FCSPs to have effective risk-based approaches, the risk-based process must be imbedded within the internal controls of the FCSP. The success of internal policies and procedures will be dependent largely on internal control systems. Two key systems that will assist in achieving this objective follow.

Culture of compliance

This should encompass:

- developing, delivering, and maintaining a training program for all FCSPs;
- monitoring for any government regulatory changes; and
- undertaking a regularly scheduled review of applicable compliance policies and procedures within accountancy practices, which will help constitute a culture of compliance in the industry.

Senior management ownership and support

Strong senior management leadership and engagement in AML is an important aspect of the application of the risk-based approach. Senior management must create a culture of compliance, ensuring that staff adheres to the firm's policies, procedures and processes designed to limit and control risks. Policies and procedures are effective only at the point that firm/company owners and senior management support the policies.⁶

⁴ These procedures are mandated by Recommendations 5, 6, 8-11, 12 and 16 of the FATF's 40+9 Recommendations

⁵ See FATF Money Laundering Typologies, http://www1.oecd.org/fatf/FATDocs_en.htm#Trends

⁶ See FATF, RBA Guidance for Trust and Company Service Providers, 17 June 2008, <http://www.oecd.org/dataoecd/19/44/41092947.pdf>

V. PERIODIC INTERNAL REVIEW OF AML SYSTEMS

11. INTERNAL TESTING OF COMPLIANCE LEVELS

- 11.1 FCSPs are required to perform periodic internal reviews, the results of which should be accessible for review both by examining independent accountants and the Commission's examiners.
- 11.2 In addition to the examination programmes, periodic testing and auditing of the AML policies, procedures and controls should be undertaken. This can be a useful tool in apprising the Commission of any changes which may have occurred between examinations. Such changes may include number of facilities, staff movements, and verification of compliance with policies, procedures, and controls to counter money laundering and terrorist financing activities in relation to all their financial intermediary services. Larger FCSPs may wish to assign this role to their Internal Audit or Compliance Department. Smaller FCSPs may accomplish the same objective by introducing a regular review by their management personnel.

VI. CLIENT IDENTIFICATION/VERIFICATION (KYC)⁷ PROCEDURES

12. GUIDANCE ON A RISK-BASED KYC PROCEDURES

12.1. The objective of KYC, which is also referred to as customer due diligence, is to ensure that reasonable steps are taken to satisfy the FCSP that the client is who he claims to be and that his funds are derived from a legitimate source or are not intended to be used for terrorism. KYC procedures should also adopt a risk-based approach. FCSPs are required to incorporate into their AML risk management framework, a risk-based KYC process in conformity with the guidance set out in this **Part C**.

12.2 A risk-based approach to KYC forms part of a risk management framework for AML which latter framework is a system for managing the risk of money laundering and terrorist financing involving the identification, categorization and mitigation of such risks.

12.3 Risk Identification

12.3.1 FCSPs should ensure that they are satisfied about the following details for all of their clients, in order to be able to make a determination about the AML risk each poses:

- who the client is? Is there public information that associates this person with any known money laundering or terrorist financing activities?
- what is his business? Is this client's occupation or business activities commonly linked to money laundering or terrorist financing activities?
- where is he located? Does the client's jurisdiction apply globally acceptable AML standards?
- where does he transact business? Does the jurisdiction where this client transacts business apply adequate AML standards or is it commonly linked to money laundering or terrorist financing activities?
- what products and services does he require? Do the products and services provided to the client offer the anonymity and movement of funds commonly linked to money laundering and terrorist financing activities?

12.3.2 A similar assessment of the risks inherent in products and services offered should be carried out.

12.3.3 It is recommended that clients, products and services should be categorized based on the degree of money laundering and terrorist financing risk they pose to the FCSP.

⁷ "KYC" is the shortened form for "know your customer" or "know your client". Often, in the banking sector this same concept may be described as "customer/client due diligence" or its diminutive form "CDD".

12.4 Categorization and mitigation of Risk

12.4.1 The Commission requires FCSPs, as a minimum, to place clients and products/services into one of two risk categories i.e. **Low Risk** or **High Risk**⁸.

12.4.2 FCSPs must also ensure that their procedures include mechanisms for appropriate **risk mitigation** which involves identifying and applying client due diligence/KYC policies and procedures to effectively mitigate the money laundering risk of particular clients, products or services identified during the risk assessment process.

12.4.3 Low Risk Characteristics

12.4.3-1 Low risk clients (and products/services) are those that may have a less than average inclination for exposing the business to money laundering and terrorist financing risks. Below, a non-exhaustive list of low risk indicators for clients (and products/services) has been provided as a guide:

(i) Clients

- a central or local government agency;
- Bahamian residents whose transactions are fully serviced by salary deductions or a financing arrangement via a prudentially regulated Bahamian financial institution or a credit union registered under the Cooperatives Act;
- a financial institution in The Bahamas that is regulated by the Central Bank, Securities Commission, Office of the Insurance Commission, the Inspector of Financial and Corporate Services, the Gaming Board and a credit union registered under the Cooperatives Act⁹;
- a foreign financial institution from a jurisdiction appearing in the first Schedule to the FTRA that is regulated by a body that has equivalent regulatory and supervisory responsibilities in that jurisdiction as the Central Bank, Securities Commission, Office of the Insurance Commission, the Inspector of Financial and Corporate Services and the Gaming Board¹⁰;
- a foreign financial institution from any other jurisdiction that is regulated and subject to a licensing process in that jurisdiction by a body that has equivalent regulatory and supervisory responsibilities as the Central Bank, Securities Commission, Office of the Insurance Commission, the Inspector of Financial and Corporate Services and the Gaming Board, and which jurisdiction has been designated by the Commission to have an AML regulatory framework that is, at least equivalent to that of Bahamian law¹¹;

⁸ It should be noted that the number of categories, i.e. two (2), required by the Commission is a minimum number. Some financial institutions may have more categories but the rationale for the number of categories and the criteria for each should be clearly documented and available for review during the course of an examination.

⁹ See para. 12.4.4-5 for additional guidance

¹⁰ See para. 12.4.4-5 for additional guidance

¹¹ See para. 12.4.4-5 for additional guidance

- a publicly traded company or mutual fund listed on The Bahamas International Stock Exchange or any other Stock Exchange specified in the Schedule to the FTRR and approved by the Securities Commission;
- a regulated investment fund as defined in section 2 (1) of the Investment Funds Act, 2003 or regulated investment fund located in a country specified in the First Schedule to the FTRA and regulated by a body having equivalent regulatory and supervisory responsibilities as the Securities Commission of The Bahamas¹²; and
- a facility holder of a Bahamian dollar facility of or below fifteen thousand dollars (B\$15,000).

(ii) Products and Services

- any cash transaction of \$15,000 BSD or below that involves a payment, deposit, withdrawal, debit, repayment, encashment, exchange, or transfer of such sums.

N.B. Although these cash transactions may be considered low risk, nevertheless a FCSP must be vigilant for, and safeguard against, persons who may employ the structuring techniques outlined in Fig. 3.

12.4.3-2 **FCSPs are reminded that the low risk indicators do not remove the obligation to perform due diligence on the customer or beneficial owner concerned, whenever there is a suspicion about the identity of the facility holder or person carrying out an occasional transaction.**

12.4.4 Due diligence for Low Risk Customers/Clients

12.4.4-1 Simplified or reduced diligence is recommended for low risk clients, in all cases, to the overriding statutory obligation¹³ to carry out verification in any situation where the FCSP suspects that a transaction involves the proceeds of criminal conduct or is destined for financing terrorist activities. Simplified or reduced due diligence means that the obligation to obtain the full complement of documentary evidence normally required is relaxed.

12.4.4-2 The KYC procedures that are implemented to mitigate the risk of money laundering and terrorist financing for low risk clients/customers should do the following in accordance with the guidance set out in section 13¹⁴ –

- identify the direct client;
- verify the client’s identity;
- identify the person with beneficial ownership and control (if different from the direct client);
- verify the identity of the beneficial owner;

¹² See para. 12.4.4-5 for additional guidance

¹³ Section 10A, FTRA

¹⁴ Section 13 sets out guidance on the details and documentation that should be obtained.

- require the conduct of on-going due diligence and scrutiny (requiring knowledge of client's business); and
 - verify the source, or intended destination of funds, as the case may be.
- 12.4.4-3 The procedures require a FCSP to establish to its satisfaction that it is dealing with a legitimate person (natural, corporate or legal) and verify the identity of those persons who have authority to conduct business through any facility provided. Whenever possible, the prospective customer should be interviewed personally.
- 12.4.4-4 Ultimately, simplified due diligence procedures should ensure that the FCSP is satisfied about the identity and existence of the customer/client; that the proper authorisations exist for the financial intermediary service being sought by the customer/client, including that the person seeking to conduct the affairs of the entity, in a relevant case, is duly authorised to do so.
- 12.4.4-5 Additional guidance on due diligence for regulated financial institution clients to which simplified due diligence may be applied under Reg. 5A of the FTRR.
- 12.4.4-5(a) For regulated financial institutions (both local and foreign), it is recommended that the confirmation of their existence and regulated status be checked by the following means:
- checking with the relevant regulator or supervisory body;
 - checking with another office, subsidiary or branch in the same country;
 - checking with a regulated bank of the institution if it is an overseas institution; and
 - obtaining from the relevant institution evidence of its licence and its authorization to conduct the financial intermediary service business with the FCSP.
- 12.4.4-5(b) In addition, the FCSP is required to satisfy itself that the regulated financial institution is subject to AML supervision that is equivalent to or exceeds standards under Bahamian law.
- 12.4.4-5(c) **N.B. Where simplified due diligence is applied to satisfy record-keeping obligations, the file should contain adequate documentation including, in appropriate cases, a copy of the relevant certificate or license or such similar document that supports the application of simplified due diligence, as well as other relevant copies of substantiating evidence.**
- 12.4.4-6 Special circumstances where simplified due diligence may be applied in the case of a previous or existing client/customer
- 12.4.4-6(a) There are two circumstances in which a FCSP may apply reduced due diligence procedures for a client that would otherwise be subject to full due diligence. This is where the FCSP may already have the necessary information in its files. The two circumstances are:

- (1) where the FCSP has reasonable grounds to believe that in relation to a particular client, the verification information/details/documentation which it has obtained on an earlier occasion is still reasonably capable of establishing the identity of that client; and
- (2) where the client is an existing one, who closes a facility and then establishes another with the FCSP, in which case the existing records may be transferred to the new facility.

12.4.4-6(b) **N.B. However, the opportunity should be taken to confirm the relevant customer verification information. This is particularly important where there has been no recent contact or communication with the client or when a previously dormant facility is being reactivated.**

12.4.5 ***High Risk Characteristics***

12.4.5-1 High-risk clients (and products or patterns) are those that may have a greater than average inclination for exposing the business to money laundering and terrorist financing. The potential for high-risk is derived, for example, from the anonymity provided by third party transactions; or that the client may originate from or reside in a crime intensive geographical location; or that the products and services are known to be conduits for money laundering and terrorist financing. Some examples of indicators for high-risk clients appear below:

(i) Clients

- financial service intermediaries that are not subject to regulation that includes a licensing requirement;
- intermediary arrangements where the real or beneficial owner of the funds is not the facility holder- i.e. anonymity factor;
- persons not ordinarily resident in The Bahamas;
- persons resident in or maintaining trading operations in locations that are known to have organized crime environments;
- persons resident in or maintaining trading operations in known drug producing/transshipment locations;
- persons from or maintaining trading operations in locations that are experiencing political instability or with a history of such;
- persons from or maintaining trading operations in locations that are designated by their relevant national authorities as high intensity financial crime areas or such similar designation;
- persons from jurisdictions where the AML regulatory framework does not meet the standards provided for under Bahamian law; and
- politically exposed persons (PEPs) - see para. **12.4.6** for further details on dealing with a PEP.

(ii) Products or Transactions

- products that involve large cash transactions over \$15,000;
- non-face to face financial transactions - financial intermediary services provided by means other than face-to-face pose a particular set of risk. Non-face-to-face transactions expose a FCSP to fraudulent activities such as identity theft. FCSPs should exercise caution when facilitating such transactions. Special care should be taken, to the extent possible, to obtain documentary evidence in relation to all parties involved in these transaction;
- products which allow customers to easily receive cash back; and
- products or services which easily allow customers to move high value items from one jurisdiction to another.

12.4.5-2 The FCSP should also ensure through its procedures that necessary measures to prevent the misuse of technological developments to facilitate money laundering or terrorist financing are in place.

12.4.6 *Enhanced Due Diligence for High Risk Customers/Clients*

12.4.6-1 In addition to the due diligence procedures for low risk customer/clients (see para. **12.4.4** above), a FCSP is required to perform enhanced due diligence in those circumstances where it knows or suspects that there is a greater propensity for illicit activity. This should become evident during the course of a risk categorization exercise where certain persons, products or services are deemed high risk.

12.4.6-2 The following activities (in addition to obtaining the verification information, evidence and documents required by Section **13**) should form part of the FCSP's enhanced due diligence procedures in order to determine the circumstances in which a client is deemed to be high risk.

(1) *Determining when the client is a high risk*

Establish procedures to determine when, either during the establishment of the business relationship, or during the course of the relationship, the person is deemed high risk.

(2) *Set an approvals hierarchy for establishing relationships with high risk clients depending on the size and management structure of the FCSP*

In the case of larger FCSPs, in addition to the MLRO, approval should be obtained from Senior Management to:

- a) establish the business relationship;
- b) continue the relationship with the person who subsequent to establishing the relationship, is found to be high risk; and
- c) continue the business relationship with a person who, subsequent to establishing the relationship, becomes high risk.

- (3) *Develop a profile of the high risk client and ascertain the expected activity.* This profile should be regularly reviewed and updated as necessary.

The process of determining a high risk profile would include how to deal with clients from jurisdictions whose AML standards are not equivalent to the requirements found in Bahamian law. In the case of PEPs this is particularly important when dealing with clients from high risk jurisdictions e.g. 'High Intensity Financial Crimes Area' in the United States and areas that are undergoing political instability or that have a history of such.

- (4) *Maintain on-going monitoring of transactions for high risk clients*

The FCSP should ensure that all transactions are closely monitored on an ongoing basis. The procedures for monitoring high-risk clients should be reasonably capable of detecting any changes in the way the facility is being operated.

12.4.6-3 Additional caution when dealing with Politically Exposed Persons (PEPs) (a special category of high risk client)

- 12.4.6-3(a) FCSPs are cautioned that PEPs may expose their businesses to significant risks. These risks whether reputational, legal etc. can be extremely detrimental and costly. Such incidences usually occur when these persons abuse their public office.

- 12.4.6-3(b) **N.B. Depending on the diversity in size and the type and volume of financial intermediary services of the FCSP, certain aspects of the high-risk client procedures may not be applicable in all cases.**

13. VERIFICATION DETAILS AND DOCUMENTARY EVIDENCE PROCEDURES

13.1 When must verification take place?

13.1.1 FCSPs have a statutory obligation to verify the identity of both low risk and high risk clients. A summary of the verification triggers required by the law are:

- when a new facility is being opened;
- when a facility holder is being added to an existing facility;
- where there is any doubt about the identity of, or the veracity or adequacy of previously obtained customer identification data on, a facility holder;
- where someone that is not your facility holder seeks to conduct a cash transaction involving \$15,000 or more either for himself or on someone else's behalf;
- where the facility holder on behalf of a third party seeks to conduct a cash transaction of \$15,000 or more using his (the facility holder's) facility;
- where there is suspicion that funds tendered as part of a transaction (cash or otherwise) are the proceeds of crime;
- where there is a material change in the way the facility is being operated.
- where there is cause to suspect that the identity of the facility holder or beneficial owner or the person conducting a transaction is in doubt;
- where there has been no recent contact with the facility holder or no transaction involving the facility within a period of 5 years, and the facility has not been closed out, the FCSP is required, by law, to verify the identity of the facility holder; and
- where structuring of an occasional transaction is suspected to be taking place. (See **Fig. 3** below for an explanation of structuring).

Figure 3: Structuring

What is structuring?

Structuring transactions as a means of avoiding having to provide verification evidence is a practice known in money laundering schemes. This structuring, which is referred to as “linked” transactions or “smurfing”, presents special challenges for verification **prior** to the transaction being conducted. For this reason there is a need in some cases to aggregate linked transactions to identify those who might structure their business activities to avoid the identification procedures.

There is no legal requirement to establish additional systems specifically to identify and aggregate linked transactions. However, where an FCSP detects that two or more cash transactions by or on behalf of someone who is not the FCSP’s facility holder, have totalled more than \$15,000, and it has reasonable grounds to suspect that this was intentionally done to avoid meeting the \$15,000 threshold that would require verification, then this information must be acted upon as soon as practicable after the FCSP forms that conclusion. The FCSP is then under an obligation to verify the identity of the person seeking to conduct any other related transaction.

The attempt to transact the linked activities must be in relation to the FCSP’s financial intermediary services, which generates the obligation to verify identity.

This requirement exists whether or not the person conducting the transaction is doing so for himself, on behalf of someone else, or in concert with others.

Timing of verification in structured transactions

Verification of identity in a structured transaction must take place as soon as reasonably practicable after concluding that structuring is taking or has taken place.

Where the person conducting the transaction under a structured arrangement is doing so through his own facility as an intermediary on behalf of someone else, the FCSP must verify the identity of that other person as soon as reasonably practicable after concluding that structuring is taking or has taken place.

Indications that transactions are being structured

In determining whether or not transactions are or have been structured to avoid the verification procedure, the FCSP shall take into consideration the following factors:

- (a) the time frame within which the transactions are conducted; and
- (b) whether or not the parties to the transactions are the same person, or are associated in any way.

13.1.2 Documentary evidence sufficient to establish the identity of the client/customer must be on record, as part of the due diligence process, for every facility or occasional transaction that has been verified for both low risk and high risk clients.

13.1.3 Regulations 3, 4 and 5 of the FTRR provide a list of mandatory documentation and information that must be obtained to verify identity, as well as additional information that may be relied upon to further establish, conclusively, the identity of a person that must be verified. The determination of any additional information required for high risk clients should be documented in the FCSP’s enhanced due diligence procedures for high risk clients.

13.2 Verification information and documents for individuals

13.2.1 *Mandatory requirements to verify an individual:-*

full and correct name, permanent address, date and place of birth, purpose of the facility, potential activity involving the facility and written confirmation that all credits to the facility are and will be beneficially owned by the facility holder, except in the case of a facility that will be an intermediary facility as verification of beneficial ownership will have to be completed separately.

13.2.2 *Additional documentation and details that may be relied upon, as deemed necessary, (based on the FCSP's risk-rating procedures) to verify an individual:*

nationality, occupation and name of employer (if self-employed, the nature of the self-employment), copy of relevant pages of passport, national identity card, voter's card, driver's licence or any other photographic identification; signature; telephone and fax number, source of funds; and such documentary or other evidence as is reasonably capable of establishing the identity of the person.

13.2.3 *Additional means of identification for non-resident clients*

13.2.3-1 A useful means of identification for non-residents is a social security, social insurance or national insurance number. FCSPs are encouraged to record such information as part of the client profile.

13.3 Verification information and documents for corporate bodies

13.3.1 *Mandatory requirements for verifying corporate entities including those that are NPOs, whether incorporated in The Bahamas or elsewhere:-*

- a. certified copy of the Certificate of Incorporation;
- b. Resolution of the Board of Director authorizing the opening of the account and conferring authority on the person who will operate the account;
- c. documentary evidence in accordance with paragraph **13.2.1** in respect of the individual identified in sub-paragraph (b) above;
- d. confirmation that the corporate entity has not been struck off the register or in the process of being wound up;
- e. written confirmation that all credits to the facility are and will be owned by the client corporate entity except in the case of a facility that will be an intermediary facility in which case the beneficial ownership identification information will have to be provided separately;
- f. names and addresses of all beneficial owners (**the obligation to verify the identity of beneficial owners shall only extend to those with a 10% controlling interest in the corporate entity**); and
- g. purpose and intended nature of the business relationship.

- 13.3.2 *In addition to the requirements above, the following information and documents may also be relied upon to support verification of a corporate entity:*

certified copy of the Memorandum and Articles of Association (or equivalent)¹⁵; location of the registered office or agent; names and addresses of all officers and directors; description and nature of the business including date of commencement of business, products and/or services provided and location/address of principal business; the potential parameters of the facility including size, in the case of investment and custody accounts, balance ranges, in the case of deposit accounts and the expected transaction volume of the account; and such other official document and other information as is reasonably capable of establishing the structural information of the corporate entity.¹⁶

- 13.3.3 The FCSP must also take reasonable measures to determine the natural persons who control the management of the corporate entity and its ownership structure.

13.3.4 ***General guidance on the process for verifying corporate entities.***

- 13.3.4-1 As a rule of thumb, the FCSP should verify the legal existence of the applicant company and ensure that any person purporting to act on behalf of the company is fully authorized. One of the principal requirements is to look behind the corporate entity and obtain the names and addresses of beneficial owners, except in those cases where reduced or simplified due diligence might apply - (see paragraphs **12.4.3** and **12.4.4** (low risk clients) and **14** (third party introductions)). Enquiries should also be made to confirm that the company exists for a legitimate trading or economic purpose and that it is not merely a “shell company” where the controlling principals cannot be identified.
- 13.3.4-2 Before a facility is established, a company search and/or other commercial enquiries should be carried out to ensure that the applicant company has not been, or is not in the process of being dissolved, struck off, wound-up or terminated.
- 13.3.4-3 If changes to the company structure or ownership occur subsequently, or if suspicions are aroused by a change in the nature of the business transacted or the profile of payments on behalf of a company, further checks should be made to ascertain the reason for the changes.
- 13.3.4-4 In appropriate cases for established businesses, a copy of the latest report and accounts (audited where applicable) should be obtained.
- 13.3.4-5 A search of the file at the local Companies Registry or the firm’s registered office is advisable, similarly an enquiry may be made via a business information service or an undertaking obtained from a firm of lawyers confirming that the constituent documents have been submitted to the Registrar of Companies.
- 13.3.4-6 When signatories to the facility change, care should be taken to ensure that the relevant authorisation from the company as well as the full name and addresses of the new signatories along with other supporting information as required by para. **13.3.1 – 13.3.3** above are obtained for the file. In addition, it may be

¹⁵ In the case of a Bahamian incorporated company, if the FCSP has, as part of the files, the documents of incorporation (e.g. certificate, Memorandum and Articles of Association) bearing an original seal of the Registrar General this would be sufficient to meet this obligation.

¹⁶ N.B. References to “account” should be construed to mean the facility or financial intermediary service that is being provided to the client facility holder.

appropriate to make periodic enquiries to establish whether there have been any changes to directors/shareholders or to the original nature of the business/activity. Such changes could be significant in relation to potential money laundering activity even though authorised signatories have not changed.

13.3.5 ***Additional guidance for due diligence in the case of foreign corporate entities.***

13.3.5-1 Since standards of control vary between different countries, careful attention should be paid to the place of origin of the verification documents and the background against which they are produced. Where appropriate, certified translations of these documents should be **obtained in English.**

13.4 Verification information and documentation for partnerships and other unincorporated associations/businesses

13.4.1 Mandatory requirements for verifying the identity of partnerships or other unincorporated businesses, including any NPOs formed by these means, the following information/documents shall be required:

- a) verification of all partners or beneficial owners in accordance with para. **13.2**;
- b) copy of partnership agreement (if any) or other agreement establishing the unincorporated business;
- c) mandate from the partnership or beneficial owner authorizing the opening of the facility and conferring authority on those who will operate the facility on behalf of the partnership or unincorporated business;
- d) documentary evidence in accordance with para. **13.2.1** in respect of the individual identified in paragraph (c) above;
- e) written confirmation that all credits to the facility are and will be beneficially owned by the facility holder except in the case of a facility that will be an intermediary facility as verification of the beneficial ownership will have to be completed separately; and
- f) purpose and intended nature of the business relationship.

13.4.2 *In addition to the above, the following information/documents may also be relied upon to complete the verification of the partnership or other unincorporated business:*

details regarding the description and nature of the business including: date of commencement of the business, products or services provided and location/address of principal place of business; potential parameters of the facility including size in the case of investment and client accounts, balance ranges in the case of deposit and client accounts and the expected transaction volume of the account; and such documentary or other evidence as is reasonably capable of establishing the identity of the partners or beneficial owners.

- 13.4.3 **General guidance on the process for verifying partnerships, clubs, societies and charities and other entities which are not incorporated**
- 13.4.3-1 Each partner or beneficial owner of the business, as the case may be, must be verified as an individual in accordance with section **13.2** above.
- 13.4.3-2 In the case of facilities to be opened for partnerships, clubs, societies and charities and other entities which are not incorporated, a FCSP should satisfy itself as to the legitimate purpose of the entity by requesting sight of the constitution or by-laws, partnership agreement etc., as the case may be, and a copy thereof placed on the file. The names and addresses of all signatories to the facility should be verified initially, as well as a written mandate from the facility holders for the signatories to act on their behalf. In addition, when signatories change, care should be taken to ensure that this information is obtained before any new signatory is permitted to conduct business on behalf of the facility holder.
- 13.5 Verification of facilities/accounts for intermediaries¹⁷ (nominees, fiduciaries, trustees etc.).**
- 13.5.1 Where a transaction is being conducted by a person in his capacity as an intermediary, including a nominee or a fiduciary on behalf of another or others, those others, unless exempted, must also be verified in accordance with the above specifications set out in paragraphs **13.2** to **13.4**. The details and documents relied upon to verify those other individuals should also be contained in the file of the primary verification subject in accordance with guidance contained in paragraph **13.2**.
- 13.6 Additional guidance on verification requirements in the case of trusts**
- 13.6.1 **N.B.: occupational pension schemes which do not allow public participation and which are registered locally under the Superannuation and Other Trusts Funds (Validation Scheme) Act¹⁸, are exempted from the verification requirements under the FTRA.**
- 13.6.2 Typologies have shown the trust to be a popular vehicle for money laundering. Particular care needs to be exercised when these arrangements have been set up in locations with strict secrecy or confidentiality rules regarding disclosure of beneficial and other such information.
- 13.6.3 Trustees should be asked to state from the outset the capacity in which they are operating or making the application for a facility. Sight of certified extracts covering the appointment and powers of the trustees from/or the original trust deed, and any subsidiary deed evidencing the appointment of current trustees, should also be obtained.
- 13.6.4 Any application to become a facility holder or undertake a transaction on behalf of another, without the applicant identifying their trust capacity, should be regarded as suspicious and should lead to further enquiries.
- 13.6.5 Where a person who makes a request to become a facility holder or to undertake a transaction does so as a professional adviser, business or company acting as trustee or nominee in relation to a third party, the FCSP must verify the identity

¹⁷ Regulation 7A, FTRR.

¹⁸ Chapter 178, 2004 Bahamas Statute Laws

of the trustee, nominee or fiduciary and the nature of their trustee or nominee capacity or duties. Enquiries should be made as to the identity of all parties for whom the trustee or nominee is acting including the settlor and any beneficiaries (except where an occasional transaction is being conducted on the beneficiary's behalf) and confirmation sought that the source of funds or assets under the trustee's control are from a legitimate source. In addition to verifying the trustee in accordance with this section, the settlor and any contributor to the trust should also be verified in accordance with this section.

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

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

13.7 Verification When Providing Safe Custody and Safety Deposit Boxes

13.7.1 Particular precautions need to be taken in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such arrangements are made available to non-clients, the identification procedures set out in this Code should be followed.

13.8 Verification of unverified pre-2001 facilities¹⁹

13.8.1 In 2004, the Commission instructed all financial institutions within its supervisory scope to verify all facilities using the risk-based approach to AML. Hence, they were required to obtain all outstanding documents/information necessary to complete the verification on of their clients on record prior to 2001. Where the institutions were not able to secure the requisite documentation, they were instructed to do the following:

- (i) document all efforts employed by the financial institution to secure the required documents;
- (ii) produce a list of unverified facilities which should be categorized as either 'low risk' or 'high risk', for review by the Commission and appointed examiners during the examination process; and
- (iii) where facilities have been designated as 'high risk', the institution should have considered filing a report with the Financial Intelligence Unit.

¹⁹ The FTRA 2000, which became law on 1st January 2001, prohibited the opening of any new facility or the provision of financial services without first having satisfied all verification obligations in respect of the prospective client. However, transitional provisions were put in place for pre-2001 facilities to be brought into compliance with the verification requirements.

13.9 Guidance on confirming the identity of a client

- 13.9.1 Although the primary duty to verify identity using the best evidence and means available rests with the FCSP; in exceptional circumstances a FCSP may wish to approach an eligible introducer, specifically for the purpose of satisfying itself on a verification of identity that it must complete. In these exceptional circumstances, the standard format set out in **Appendix F** should be used for making the enquiry.

13.10 Guidance on verifying address

- 13.10.1 In addition to the name verification, it is important that the current permanent address should also be verified. Any current documentation or identification issued by a valid government or public authority may be relied upon to establish this. It is sufficient for the officer or employee conducting the verification to certify that he has seen and is satisfied with the evidence relied upon to verify the address. It is not necessary to keep copies of documentation that establishes the permanent address, just for that purpose.

14 THIRD PARTY (OR ELIGIBLE) INTRODUCTIONS

14.1 The ultimate responsibility for verifying the identity of a client rests with the FCSP. However, in certain circumstances and in accordance with the guidance in this section, a FCSP may rely on either, on the due diligence carried out by a third party (eligible introducer) to satisfy its primary duty to verify identity.

14.2 **N.B. This exception from having to obtain full verification documentation is subject to the overriding statutory obligation²⁰ to carry out verification in any case where the FCSP suspects that a transaction involves the proceeds of criminal conduct or is destined for financing terrorism.**

14.3 What Is An Eligible Introducer?

14.3.1 An eligible introducer is any one of the following:

- in the case of The Bahamas any other financial institution under section 3 of the FTRA ; or
- any foreign financial institution from a jurisdiction in **Appendix B** that is regulated by a body having equivalent regulatory and supervisory responsibilities as the Central Bank, the Securities Commission, the Office of the Insurance Commission, the Inspector of Financial and Corporate Services and the Gaming Board; or
- any other foreign financial institution from a jurisdiction outside of The Bahamas which has been designated by the Commission as having an equivalent or better AML regulatory framework to that which exists under Bahamian law and which is also regulated by a body having equivalent regulatory and supervisory responsibilities as the Central Bank, the Securities Commission, the Office of the Insurance Commission, the Inspector of Financial and Corporate Services or the Gaming Board.

14.3.2 FCSPs must satisfy themselves prior to establishing the facility that the eligible introducer meets the specified requirements set out in the paragraph above.

14.3.3 ***Circumstances in which the FCSP may rely on a verification carried out by an eligible introducer to satisfy its primary obligation to verify a client***

14.3.3-1 Permissible eligible introductions where a facility is being established

14.3.3-1(a) In the case of facilities, eligible introductions are permitted in the following circumstances-

- i. *Establishment of facilities by telephone, Internet or post.*

A FCSP can establish a facility by means of telephone, Internet or post where a letter of introduction stipulating that the eligible introducer has verified the prospective client is provided. If the client has been introduced by this means, an original letter on file should reflect this fact.

²⁰ Section 10A, FTRA

ii. *Arrangements between Existing Facilities*

In the case of arrangements between two facilities which accommodate the conduct of transactions between them (whether held by the same or different financial institutions), the duty to verify identity is met once all such steps as are reasonably necessary to confirm the existence of the other facility have been taken. For example, where a client engages the services of a FCSP to receive periodic deposits on its behalf from an account it (the client) has at an eligible introducer bank, the FCSP may rely on the fact that it has confirmed the existence of such a facility, to discharge its primary obligation to verify. The records to be maintained in this situation are those that are reasonably necessary to enable the identity of the other eligible introducer (in this case the bank), the identity of the facility and the identity confirmation of the person; and

iii. *Corporate Group Introductions*

Reliance may be placed on the verification carried out by another FCSP of a group that is a subsidiary or parent of which the FCSP is a member and which is subject to an AML group policy, that is strictly adhered to, and which is at least consistent with the standards provided by Bahamian law, for the purpose of introducing a prospective client wishing to establish a facility in The Bahamas.

14.3.3-1(b) Where a facility has been established by any of the foregoing means, there is no need to carry out an independent verification of the client. However, the FCSP is obliged to obtain and have on record an original letter from the eligible introducer:

- containing information which identifies the facility holder and any beneficiaries or relevant beneficial owners, his (the facility holder) authority to act in those cases where he is not the ultimate beneficial owner and the purpose and intended nature of the business relationship; and
- advising that it (the eligible introducer) has verified the client being introduced and is in possession of the necessary verification information and documentary evidence sufficient to satisfy the requirements of the Bahamian AML laws. The letter from the eligible introducer must also provide an undertaking to supply to the FCSP upon request, immediately and without delay, copies of such evidence and documentation.

14.3.2-1 (c) In appropriate circumstances the FCSP may also seek to obtain directly from the client details regarding the source of income/funds, purpose, use, potential activity and other parameters for the operation of the facility, and document these.

14.3.2-2 Permissible eligible introductions where an occasional transaction (i.e. sums in excess of the \$15,000 threshold) is being attempted/conducted.

14.3.2-2 (a) An occasional transaction is one in which the sum involved exceeds \$15,000 and where the person purporting to conduct the transaction, or on whose behalf the transaction is being conducted, is not a facility holder of the FCSP.

14.3.2-2 (b) Letters of Confirmation may be used to satisfy the primary obligation on a FCSP to verify identity, when a sum in excess of \$15,000 is involved in a transaction being conducted by or on behalf of a non-facility holder.

14.3.2-2 (c) Only eligible introducers can issue Letters of Confirmation, i.e. those entities outlined in section **14.3.1** above.

14.3.2-2 (d) The circumstances involving an occasional transaction in which reliance may be placed on a letter of confirmation issued by another eligible introducer financial institution certifying that it (the eligible introducer financial institution) has carried out the required verification are as follows:

- (1) where a deposit is made into a facility that is provided for the FCSP by an eligible introducer financial institution and the FCSP is unable to determine if such a deposit involved an occasional transaction. An example of this is where a facility holder client makes a deposit directly into a bank account of the FCSP, then the FCSP can rely on written confirmation from the bank that it (the Bank) has carried out the verification of the person making the deposit;
- (2) reliance can be placed on written confirmation of an eligible introducer e.g. a bank, which conducts a cash transaction of \$15,000 or more on behalf of another person with the FCSP that it (the bank) has carried out the required verification on the party on whose behalf it is acting; and
- (3) a FCSP can rely on a written confirmation from an eligible introducer (e.g. a bank) that it (the bank) has carried out the required verification on a non-facility holder who has conducted an occasional transaction with the FCSP by means of a facility which that verification subject has with the bank. The records to be kept in such eventuality should indicate:
 - the identity of the eligible introducer,
 - the identity of that facility, and
 - the identity confirmation of the person.²¹

²¹ Section 11 (4), FTRA.

15. MONITORING OF FACILITIES

- 15.1 FCSPs are expected to maintain systems and controls in place to monitor, on an ongoing basis, the relevant activities in the course of the business relationship to ensure consistency with stated facility purposes and activities. The nature and sophistication of this monitoring will depend on the nature of the business. The purpose of this monitoring is for FCSPs to be vigilant for any significant changes or inconsistencies in the pattern of transactions, having regard to, amongst other things, its knowledge of the customer, its business and risk profile and where necessary, the source of funds. Inconsistency is measured against the stated original purpose of the facility. Areas to monitor could be:
- (a) transaction type
 - (b) frequency
 - (c) amount
 - (d) geographical origin/destination
 - (e) facility signatories
- 15.2 It is recognized that the most effective method of monitoring facilities is achieved through a combination of computerized and human manual solutions. A corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with customers, will form an effective monitoring method as a matter of course.
- 15.3 FCSPs should, to the extent possible, examine the circumstances of complex and unusual, large transactions or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose and document their findings and maintain such information for a minimum period of five years.
- 15.4. Having regard to the size, volume of financial services business and complexity of such business, FCSPs should ensure that documents, data or information collected under the due diligence process is kept up-to-date and relevant, through periodic reviews of existing records, particularly for high risk clients. The process by which records are kept current should be documented as part of the record-keeping policies.

VII. RECORD KEEPING PROCEDURES

16. Statutory requirements to maintain records

16.1 FCSPs are required to retain records concerning customer identification and transactions for use as evidence in any investigation into money laundering or terrorist financing. This is an essential component of the audit trail procedures. Often, the only significant role a financial institution can play in an investigation is through the provision of relevant records, particularly where the money launderer or person financing terrorism has used a complex web of transactions specifically for the purpose of confusing the audit trail. The objective of the statutory requirements detailed in the following paragraphs is to ensure, in so far as is practicable, that in any subsequent investigation, the FCSP can provide the authorities with its part of the audit trail.

16.2 Where an obligation exists to keep records, copies of the relevant documentation are sufficient, unless the law specifically requires otherwise. It is important that the FCSP satisfies itself that copies are reproductions of the original documentation. The files should also indicate, in relevant circumstances, where the original can be located.

16.3 The records prepared and maintained by any FCSP on its customer relationships and transactions should be such that:

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

16.4 Format of records

16.4.1 Retention of verification and transaction records may be by way of original documents, stored on microfiche, computer disk or in other electronic form.

16.5 Identification/verification (KYC) records

16.5.1 Section **13** sets out the evidence to be obtained for verification of identity.

16.5.2 For the purpose of verifying the identity of any person a FCSP must keep such records as are reasonably capable of enabling the FIU to readily identify the nature of the evidence used for the verification.

16.5.3 Verification records for eligible introductions involving the confirmation of the existence of a facility

16.5.3-1 Where a FCSP verifies the identity of any person by confirming the existence of a facility provided by an eligible introducer financial institution, the records that must be retained are such that enable the FIU to identify, at any time, the identity of the eligible introducer financial institution, the identity of the relevant facility and the identity confirmation documentation of the verification subject.

16.5.4 Retention period for verification records

- 16.5.4-1 In relation to any other person, records relating to the verification of the identity of any person must be kept for a period of not less than 5 years after the verification was carried out.
- 16.5.4-2 Records relating to the verification of the identity of facility holders must be retained for 5 years after the person ceases to be a facility holder. In keeping with best practices, the date when a person ceases to be a facility holder is the date of:
- i) the carrying out of a one-off transaction or the last in the series of transactions; or
 - ii) the ending of the business relationship, i.e. the closing of the facility; or
 - iii) the commencement of proceedings to recover debts payable on insolvency.
- 16.5.4-3 Where formalities to end a business relationship have not been undertaken, but a period of 5 years has elapsed since the date when the last transaction was carried out, then the five-year retention period commences on the date of the completion of the last transaction.
- 16.5.4-4 Records relating to the verification of the identity for any transaction conducted through a facility of an intermediary must be kept for a period of not less than 5 years after the intermediary ceases to be a facility holder.
- 16.5.4-5 Where records relate to on-going investigations, they must be retained until it is confirmed by the FIU or local law enforcement agency that the case has been closed.

16.6 Transaction records

- 16.6.1 The investigating authorities also need to be able to establish a financial profile of any suspect facility. For example, in addition to information on the beneficial owner of the facility and any intermediaries involved, the volume of funds flowing through the facility may be sought also as part of an investigation into money laundering or terrorism. Further, in the case of selected transactions, information may be required on the origin of the funds (if known); the form in which the funds were offered or withdrawn, i.e. cash, cheques, etc., the identity of the person undertaking the transaction, the destination of the funds, and the form of instruction and authority.
- 16.6.2. The transaction records which must be kept must include the following information:
- the nature of the transaction;
 - the amount of the transaction, and the currency in which it was denominated;
 - the date on which the transaction was conducted;
 - the parties to the transaction;
 - where applicable, the facility through which the transaction was conducted, and any other facilities (whether or not provided by the FCSP) directly involved in the transaction; and

- all other files and business correspondence and records connected to the facility.

16.6.3 Transaction records to be kept for a minimum period of five (5) years

16.6.3-1 Transaction records must be kept for a minimum period of five years after the transaction has been completed, subject to the extended requirements where the records relate to an ongoing investigation then they must be retained until it is confirmed by the FIU or local law enforcement agency that the case has been closed.

16.7 When records need not be kept

16.7.1 Special considerations for record retention on the liquidation of a financial institution

16.7.1-1 Nothing in sections 23, 24 or 25 of the FTRA require the retention of any records kept by a financial institution, being a company, in any case where that financial institution has been liquidated and finally dissolved. However, the liquidator of the financial institution is required to maintain for the balance of the prescribed period remaining at the date of dissolution such records that would otherwise have been required to be kept by the financial institution but for the liquidation.

16.8 Destruction of Records

16.8.1 The records and any copies thereof, maintained pursuant to the FTRA must be destroyed as soon as practicable after the expiration of the retention period, unless required to be maintained beyond this period by any law, for the business purposes of the FCSP, or for investigative purposes by law enforcement or the FIU.

VIII. PROCEDURES FOR THE RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

17 THE FINANCIAL INTELLIGENCE UNIT (FIU)

- 17.1 The national agency for receiving suspicious transaction reports (STRs) is the Financial Intelligence Unit, Norfolk House, Frederick Street, P.O. Box SB-50086, Nassau, The Bahamas, Telephone # (242) 356-9808 or (242) 356-6327, Fax # (242) 322-5551, **website:** www.bahamas.gov.bs/fiu.
- 17.2 The FIU has power to compel production of information (except information subject to legal professional privilege), which it considers relevant to fulfill its functions.
- 17.3 It is an offence to fail or refuse to provide the information requested by the FIU. Such offence is punishable on summary conviction to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 2 years or to both such fine and imprisonment.
- 17.4 The FIU is empowered by the FIUA to issue Guidelines, from time to time to assist financial institutions with observance and implementation of STR procedures. Copies of these Guidelines, which supplement and add to these Codes, are available from the FIU's office and electronically from the FIU's website.

17.5 Mandatory requirement to appoint a Money Laundering Reporting Officer

- 17.5.1 All FCSPs engaged in financial intermediary services are required by law²² to appoint a Money Laundering Reporting Officer (MLRO) as the point of contact with the FIU, in order to handle reports of money laundering suspicions by their staff.
- 17.5.2 The MLRO must be registered with the FIU. FCSPs should ensure that any changes in this post are immediately notified to the FIU and the Commission.
- 17.5.3 The Role of the MLRO
- 17.5.3-1 The type of person appointed as MLRO will depend on the size of the FCSP and the nature of its business, but he should be sufficiently senior to exercise the necessary authority. Larger FCSPs may choose to appoint, as appropriate to the circumstances, a senior member of their compliance department. In small FCSPs, it may be appropriate to designate the office administrator, the sole practitioner or one of the partners. When several subsidiaries operate closely together within a group, designating a single MLRO at group level is an option.
- 17.5.3-2 The MLRO is required to determine whether the information or other matters contained in the transaction report he has received give rise to a knowledge or suspicion that someone is engaged in money laundering.
- 17.5.3-3 In making this judgment, the MLRO should consider all other relevant information available within the FCSP concerning the person or business to whom the initial report relates. This may include a review of other transaction patterns and volumes through the account(s) in the same name, the length of

²² Reg. 5 of the FI(TR)R

the business relationship, and referral to identification records held. If, after completing this review, he decides that the initial report gives rise to a knowledge or suspicion of money laundering, then he must disclose this information to the FIU. It is therefore imperative that the MLRO be granted timely access to customer verification and related due diligence information, transaction records and other relevant information.

17.5.3-4 The “determination” by the MLRO implies a process with at least some formality attached to it, however minimal that formality might be. It does not necessarily imply that he must give his reasons for negating, and therefore not reporting any particular matter, but it clearly would be prudent, for his own protection, for internal procedures to require that only written reports are submitted to him and that he should record his determination in writing, and the underlying reasons therefore.

17.5.3-5 The MLRO will be expected to act honestly and reasonably and to make his determinations in good faith.

17.5.3-6 The Commission has oversight of a diverse group of business types and sizes. In practical terms, designated FCSPs may vary from the sole proprietorship to large businesses with huge organizational structures. Nonetheless, each MLRO should diligently perform the requisite duties in the most professional manner. This area will be reviewed during the on-site examination of the business.

17.5.3-7 Financial institutions supervised by the Commission are at liberty to appoint a person to serve as MLRO once they are satisfied that the individual meets at least the core competencies outlined below, i.e. the MLRO should:

- have a sound understanding of the money laundering and terrorist financing risks of his financial institution;
- have a basic knowledge of the Bahamian AML/CFT laws and rules;
- be given sufficient authority and independence to perform his duties;
- to the extent possible, be a Senior Officer within his institution; and
- be exposed to AML/CFT training at least once annually.

17.5.3-8 During the routine and/or random on-site examination, the Commission will determine whether the financial institution has complied with the above requirements.

17.6 Mandatory requirement to appoint a Compliance Officer

17.6.1 A FCSP is also required, by law, to appoint a Compliance Officer (CO). However, the FCSP may choose to combine the roles of the CO with the MLRO depending upon the size and nature of financial intermediary services that it is involved in.

17.7 Recognition of Suspicious Transactions

17.7.1 A suspicious transaction will often be one which is inconsistent with a customer’s known, legitimate business or personal activities or with the normal business for that type of facility. Therefore, the first key to recognition is knowing enough about the customer’s business to recognize that a transaction, or series of transactions, is unusual. Efforts to recognize suspicious

circumstances should commence with the request to open a facility or execute the initial transaction.

17.7.2 Section 43 (2) of the POCA requires that any person who knows, suspects or has reasonable grounds to suspect that another person is engaged in money laundering which is related to proceeds of drug trafficking or any related crime, and fails to report such knowledge or suspicion is guilty of an offence.

17.7.3 Under the FTRA section 14 where any person conducts or seeks to conduct any transaction by, through or with a financial institution (whether or not the transaction or proposed transaction involves funds), and the financial institution knows, suspects or has reasonable grounds to suspect that the transaction or the proposed transaction involves proceeds of criminal conduct as defined in the POCA, or any offence under the POCA, the financial institution shall, as soon as practical after forming that suspicion, report that transaction or proposed transaction to the FIU.

17.8 Internal Reporting of Suspicious Transactions

17.8.1 The FI(TR)R requires FCSPs to establish clear responsibilities and accountabilities to ensure that policies, procedures, and controls which deter criminals from using their facilities for money laundering, are implemented and maintained.

17.8.2 All FCSPs offering financial intermediary services operating within or from The Bahamas are required to:

- i. introduce procedures for the prompt investigation of suspicions and subsequent reporting of same to the FIU;
- ii. provide the MLRO with the necessary access to systems and records to fulfill this requirement; and
- iii. establish close co-operation and liaison with the FIU and the Commission.

17.8.3 There is a statutory obligation on all staff to report suspicions of money laundering to the MLRO in accordance with internal procedures. However, in line with accepted practice some FCSPs may choose to require that such unusual or suspicious transactions be drawn simultaneously to the attention of supervisory management to ensure that there are no known facts that will negate the suspicion.

17.8.4 All FCSPs have a clear obligation to ensure:

- that each relevant employee knows to which person he should report suspicions; and,
- that there is a clear reporting chain under which those suspicions will be passed without delay to the MLRO.

17.8.5 Once an employee has reported his suspicion to the MLRO, he has fully satisfied his statutory obligation.

17.9 Procedure for reporting suspicious transactions to the FIU

- 17.9.1 The form at **Appendix G** should be used for reporting suspicious transactions to the FIU, and the information should be typed²³. These disclosures can be forwarded to the FIU in writing, by hand, by post, by facsimile message or by electronic mail, and in cases of urgency, reports may be made orally. However, this should still be followed by a written report.
- 17.9.2 Sufficient information should be disclosed which indicates the nature of and reason for the suspicion. Where the FCSP has additional relevant evidence that could be made available, the nature of this evidence should also be clearly indicated.
- 17.9.3 The receipt of a disclosure will be acknowledged by the FIU. Normally, completion of a transaction will not be interrupted. However, in exceptional circumstances, such as the imminent arrest of a client and consequential restraint of assets, the FCSP may be required by the FIU to discontinue the transaction or cease activity related to the client's facility.
- 17.9.4 Following receipt of a disclosure and initial research by the FIU, if appropriate, the information disclosed is allocated to financial investigation officers in the FIU for further investigation. This is likely to include seeking supplementary information from the FCSP making the disclosure, and from other sources. Discrete enquiries are then made to confirm the basis for suspicion. The client is not approached in the initial stages of investigating a disclosure and will not be approached unless criminal conduct is identified.
- 17.9.5 Access to the disclosure is restricted to financial analysts and other officers within the FIU.
- 17.9.6 It is also recognised that as a result of a disclosure, a FCSP may leave itself open to risks as a constructive trustee if moneys are paid away other than to the true owner. The FCSP must therefore make a commercial decision as to whether funds which are the subject of any suspicious report (made either internally or to the FIU) should be paid away under instruction from the facility holder.
- 17.9.7 FCSPs are reminded that reporting to the Commission, the Central Bank, the Commissioner of Police and any duly authorized employee of the FCSP will be accorded similar protection against breach of confidentiality. It is therefore recommended that, to reduce the risk of constructive trusteeship when fraudulent activity is suspected, and to obtain the fastest possible FIU response, disclosure should be notified by telephone and the disclosure form forwarded to the FIU. Where timing is believed to be critical, a FCSP should prepare a back up package of evidence for rapid release on the granting of a Court Order, search warrant, or a freezing order pursuant to the Section 4(2)(c) of the FIUA.
- 17.9.8 Following the submission of a disclosure report, a FCSP is not precluded from subsequently terminating its relationship with the client provided it does so for commercial or risk containment reasons and does not alert the client to the fact of the disclosure which would constitute the offence of tipping off under the FTRA. However, it is recommended that, before terminating a relationship in these circumstances, the reporting institution should liaise directly with the investigation officer in the FIU to ensure that the termination does not tip off the customer or prejudice the investigation in any way.

²³ An electronic copy of the form is available from the FIU's website.

17.10 Feedback from the FIU

- 17.10.1 The provision of general feedback to the financial sector on the volume and quality of disclosures and on the levels of successful investigations arising from the disclosures will be provided on a regular basis by the FIU.
- 17.10.2 Where applicable, FCSPs should ensure that all contact between particular departments/branches with the FIU and law enforcement agencies is reported back to the MLRO so that an informed overview of the situation can be maintained. In addition, the FIU will continue to provide information on request to a disclosing institution in order to establish the current status of a specific investigation.

IX. STAFF RECRUITMENT, EDUCATION AND TRAINING PROCEDURES

18 KNOW YOUR EMPLOYEE (KYE) PROCEDURES

- 18.1 The financial services industry in The Bahamas, as in any other jurisdiction, is challenged with managing a diverse range of risks such as reputational, legal, operational etc. Consequently, in addition to financial institutions implementing proper procedures to mitigate risk from external forces, attention should also be placed on potential risks posed to financial institutions from internal forces such as from their employees. Appropriate procedures, including those for screening, should be implemented and documented for the hiring of employees. In this regard, the Commission offers some guidance to its constituent financial institutions which may be useful in managing the related risks.
- 18.2 The screening process for hiring new employees may include:
- background and employee history checks; and
 - reference checks, including police character reference (or equivalent).
- 18.3 Employers may also consider monitoring employees who display the following behavior:
- unusual transaction activities;
 - unusual increases in business activities; and
 - association with persons known to be involved in criminal activities.
- 18.4 The most effective KYE programme should be complemented by a sound on-going training programme which includes staff awareness.

19. STAFF AWARENESS PROGRAMMES

- 19.1 FCSPs must take appropriate measures to familiarize all of their employees with:
- i. policies and procedures designed to detect and prevent money laundering including those for identification, record keeping and internal reporting, and any legal requirements in respect thereof; and
 - ii training programmes which incorporates the recognition and handling of suspicious transactions.
- 19.2 Staff must be aware of their own personal AML statutory obligations including the fact that they can be personally liable for failure to report information in accordance with internal procedures. All staff should be encouraged to cooperate fully and to provide a prompt report of any suspicious transactions without fear of reprisal.
- 19.3 It is important that all FCSPs covered by this Code introduce adequate measures to ensure that staff members are fully aware of their responsibilities.

20. STAFF EDUCATION AND TRAINING PROGRAMMES

20.1 Timing and content of training for various sectors of staff will need to be adapted by individual FCSPs for their own needs. It will also be necessary to make arrangements for refresher training at regular intervals, i.e. at least annually to ensure that staff members remain current with their responsibilities.

20.2 The Commission hosts a number of AML training seminars each year for its constituents.

20.3 The following training guideline is recommended:

20.4 New employees

20.4.1 A basic training course on money laundering and terrorist financing, including relevant typologies and the subsequent need for reporting any suspicious transactions to the MLRO should be provided to all new employees within the first month of their employment. This is particularly critical for persons who will be dealing with clients or their transactions, irrespective of the level of seniority. They should be made aware that there is a legal requirement to report suspicion and that there is a personal statutory obligation in this respect. They should also be provided with a copy of the written policies and procedures in place in the FCSP for the reporting of suspicious transactions.

20.5 Frontline Staff that deal directly with the public for the purpose of receiving and making payments, deposits etc., such as cashiers/ accounts officers

20.5.1 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 organization's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and the procedures to be adopted when a transaction is deemed to be suspicious.

20.5.2 All frontline staff should be made aware of their financial institution's policy for dealing with non-clients, including those that wish to conduct a transaction in relation to a client facility holder, particularly where large cash transactions, travelers cheques or postal money orders are involved. They should be reminded of the need for extra vigilance in these cases.

20.5.3 In addition to the above, further training should be provided regarding the need to verify a customer's identity and on the business' own facility creation and customer/client verification procedures. All employees should be familiarized with the FCSP's suspicious transaction reporting procedures.

20.6 Administration/operations supervisors and managers

20.6.1 A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff in the foregoing categories. This will include the offences and penalties arising from the POCA and the FTRA for non-reporting and for assisting money launderers; procedures relating to the service of production and restraint orders; internal reporting procedures; the requirements for verification of identity; the retention of records and disclosure of suspicious transaction reports under the FIUA (See **Appendix E** for a summary of these offences).

20.7 Money Laundering Reporting Officers (MLRO)/Compliance Officers (CO)

20.7.1 In-depth training concerning all aspects of the legislation and internal policies will be required for the MLRO and the CO. In addition, these officers will require extensive initial and on-going instruction on the validation, investigation and reporting of suspicious transactions and on the feedback arrangements and on new trends and patterns of criminal activity.

SUMMARY OF BAHAMIAN LAW ON AML/CFT**The Proceeds of Crime Act, Ch. 93**

This Act criminalizes money laundering related to the proceeds of drug trafficking and other serious crimes. This Act also provides for the confiscation of the proceeds of drug trafficking or any relevant offence as described in the Schedule to the Act; the enforcement of confiscation orders and investigations into drug trafficking, ancillary offences related to drug trafficking and all other relevant offences.

The law requires persons to inform the FIU, the Police and other relevant agencies of any suspicious transactions that comes to light during the course of their employment, trade or business activities. The Act provides immunity to such persons from legal action by clients aggrieved by the breach of confidentiality. It should be noted that the reporting of suspicious transactions is mandatory and a person who fails to report a suspicious transaction is liable to prosecution.

The Financial Transactions Reporting Act, Ch. 368

The FTRA imposes mandatory obligations on designated financial institutions to: verify the identity of existing and prospective customers and clients; maintain verification and transaction records for prescribed periods; and to report suspicious transactions, which involve the proceeds of criminal conduct as defined by the Proceed of Crime Act to the Financial Intelligence Unit. This Act also establishes the Compliance Commission, an independent statutory authority which has responsibility for ensuring that designated financial institutions that are not otherwise regulated, comply with the provisions of the Act. These are outlined in Section 46 of the Act. The Act also provides for the Minister to designate a self-regulatory organization (SRO) for a profession, as the AML supervisor, on the recommendation of the Commission.

The Financial Transactions Reporting Regulations, Ch. 368

The Financial Transactions Reporting Regulations, Ch. 368, inter alia, sets out the evidence that financial institutions must obtain in satisfaction of any obligation to verify the identity of a client or customer.

The Financial Intelligence Unit Act, Ch. 367

The Financial Intelligence Unit Act, Ch. 367 establishes the FIU of The Bahamas which has power, inter alia, to receive, analyse and disseminate information which relates to or may relate to the proceeds of offences under the Proceed of Crime Act.

The Financial Intelligence (Transactions Reporting) Regulations, Ch.367

The Financial Intelligence (Transactions Reporting) Regulations, Ch. 367 requires financial institutions to establish and maintain identification, record-keeping, and internal reporting procedures, including the appointment of a MLRO and Compliance Officer. These Regulations also require financial institutions to provide appropriate training for relevant employees to make them aware of the statutory provisions relating to money laundering and impose sanctions for failure to comply with Guidelines and Codes issued by the Regulators or the FIU.

The Anti-Terrorism Act , Ch. 107 (2004 Statute laws of The Bahamas).

This Act criminalizes terrorist activities and the financing of terrorism and punishes offenders in or outside The Bahamas. It also prohibits the collecting of funds for terrorist/criminal purposes. Further, it makes persons responsible for the management or control of a legal entity that are involved with terrorist actions liable. The Act imposes a duty to report any suspicion to the Commissioner of Police regarding funds to be used to facilitate terrorism. The freezing of funds, forfeiture orders, sharing of forfeited funds and extradition that are related to terrorist movements are prescribed under the Act.

(1) APPROVED COUNTRIES UNDER THE FIRST SCHEDULE TO THE FTRA

Countries and territories from which verification by eligible introducer financial institutions may be accepted (section 15):-

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

(2) APPROVED STOCK EXCHANGES UNDER THE SCHEDULE TO THE FTRR

<p>American Stock Exchange (AMEX) Amsterdam Stock Exchange (Ainsterdamse Effectenbeurs) Antwerp Stock Exchange (Effectenbeurs vennootschap van Antwerpen) Athens Stock Exchange (ASE) Australian Stock Exchange Barcelona Stock Exchange (Bolsa de Valores de Barcelona) Basle Stock Exchange (BaslerBorse) Belgium Futures & Options Exchange (BELFOX) Berlin Stock Exchange (Berliner Borse) Bergen Stock Exchange (Bergen Bors) Bermuda Stock Exchange Bilbao Stock Exchange (Borsa de Valores de Bilbao) Bologna Stock Exchange (Borsa Valori de Bologna) Bordeaux Stock Exchange Boston Stock Exchange Bovespa (Sao Paulo Stock Exchange) Bremen Stock Exchange (Bremener Wertpapierbarse) Brussels Stock Exchange (Societede la Bourse des Valeurs Mobilieres/Effecten Beursvennootschap van Brussel) Cayman Islands Stock Exchange Cincinnati Stock Exchange Copenhagen Stock Exchange (Kobenhayns Fondsbors) Dusseldorf Stock Exchange (Rheinsch-westfililische Borse Zu Dusseldorf) Florence Stock Exchange (Borsa Valori di Firenze) Frankfurt Stock Exchange (Frankfurter Wertpapierbarse) Geneva Stock Exchange Genoa Stock Exchange (Borsa Valari de Genova) Hamburg Stock Exchange (Hanseatische Vertpapier Borse Hamburg) Helsinki Stock Exchange (Helsingen Arvapaperiporssi Osuuskunta) Hong Kong Stock Exchange Fukuoka Stock Exchange Irish Stock Exchange Johannesburg Stock Exchange Korea Stock Exchange Kuala Lumpur Stock Exchange Lille Stock Exchange Lisbon Stock Exchange (Borsa de Valores de Lisboa) London Stock Exchange (LSE) Luxembourg Stock Exchange (Societe de la Bourse de Luxembourg SA) Lyon Stock Exchange Madrid Stock Exchange (Balsa de Valores de Madrid) Marseille Stock Exchange Mexican Stock Exchange (Bolsa Mexicana de Valores) Midwest Stock Exchange</p>	<p>Milan Stock Exchange (Borsa Valares de Milano) Montreal Stock Exchange Munich Stock Exchange (Bayerische Barse in Miinchen) Nagoya Stock Exchange Nancy Stock Exchange Nantes Stock Exchange Naples Stock Exchange (Borsa Valori di napoli) NASDAQ (The National Association of Securities Dealers Automated Quotations) New York Stock Exchange New Zealand Stock Exchange Oporto Stock Exchange (Bolsa de Valores do Porto) Osaka Stock Exchange Oslo Stock Exchange (Oslo Bars) Pacific Stock Exchange Palermo Stock Exchange (Borsa Valari di Palermo) Paris Stock Exchange Philadelphia Stock Exchange Rio de Janeiro Stock Exchange (BVRI) Rome Stock Exchange (Borsa Valori di Roma) Singapore Stock Exchange Stockholm Stock Exchange (Stockholm Fondsbors) Stuttgart Stock Exchange (Baden-Wiirtembergische Wertpapierborse Zu Stuttgart) Taiwan Stock Exchange The Stock Exchange of Thailand Tokyo Stock Exchange Toronto Stock Exchange Trieste Stock Exchange (Borsa Valori di Trieste) Trondheim Stock Exchange (Trondheims Bors) Turin Stock Exchange (Borsa Valori de Torino) Valencia Stock Exchange (Borsa de Valares de Valencia) Vancouver Stock Exchange Venice Stock Exchange (Borsa Valori de Venezia) Vienna Stock Exchange (Wiener Wertpapierbarse) Zurich Stock Exchange (Ziircher Borse).</p>
--	---

THE COMPLIANCE COMMISSION
&
THE INSPECTOR OF FINANCIAL & CORPORATE SERVICE PROVIDERS

EXAMINATION FORM

FINANCIAL & CORPORATE SERVICE PROVIDERS

Section 11(3)(b) of the Financial and Corporate Services Providers Act, Chapter 369 (FCSPA) calls for mandatory inspections of the operations of Financial and Corporate Service Providers.

Under Section 15 of the FCSPA, all Financial and Corporate Service Providers (FCSPs) are required to maintain certain records of all their International Business Companies (IBCs) and Exempted Limited Partnerships. These records are examined under Section I of this form.

Section II of this form provides for the examination pursuant to the FTRA's anti-money laundering requirements and the requirements of the Anti-Terrorism Act, 2004. The facilities of each FCSP is subject to Anti-Money Laundering/ Combating the Financing of Terrorism (AML/CFT) regulation where services rendered by the licensee involve facilitating the entry or placement, movement, or removal of funds, into, within or out of the financial system on behalf of clients. If an FCSP does not provide any of the preceding financial intermediary services, then he/it is not required to complete Section II of this form.

Revised July, 2009

**THE INSPECTOR, FINANCIAL AND CORPORATE
SERVICE PROVIDERS**

Third Floor
Charlotte House
Shirley Street
P.O. Box N-532
Nassau, Bahamas

THE COMPLIANCE COMMISSION

Second Floor
Charlotte House
Shirley Street
P.O. Box N-3017
Nassau, Bahamas

Instructions

Please read all instructions carefully before completing this form

What is the purpose of this form?

The purpose of this form is to assess the level of compliance of financial institutions with the requirements of Bahamian AML/CFT laws and rules.

Who should complete this form?

This form may be used by the Compliance Commission and Accountants duly appointed to act as agents of the Commission in the conduct of On-Site Examinations. This form may also be used by a senior staff member of a financial institution for the purpose of an Off-Site Examination.

Please indicate below the type of examination to be conducted:

Compliance Commission Examiner

Follow-up On-Site Examination
Random On-Site Examination
Special On-Site Examination

Appointed Accountant

Routine On-Site Examination

Authorized Senior Staff Member of Financial Institution

Routine Off-Site Examination

If this is an Off-Site, please state the name and position of person completing the form

Name

Position

Notes to the Examiner:

1. This examination form is in two parts - the first Section relates to the regulatory obligations of the FCSPA while the second Section relates to obligations of the FTRA. Section II of this form should only be completed if a Financial and Corporate Service Provider has facilities through which a facility holder may place, move, or remove funds, into, within or out of the financial system.
2. Examiners are reminded that all examinations are risk-based. Where the financial institution has not categorized its facilities into high or low risk for money laundering and terrorist financing, the examination **should not** be completed. Please advise the Commission of this immediately.
3. Examination forms should be type-written and returned to the Compliance Commission within ten (10) working days subsequent to the completion date of the examination.
4. **The examination year commences 1st January of each year and ends 31st December of the following year.**
5. Definition of key terms on the examination form can be found on page 11 of this form and a sample guide can be found on page 12.

PART II
VERIFICATION AND RECORD-KEEPING OBLIGATIONS

10. Number of International Business Companies (IBCs) on record: _____

11. Number of Exempted Limited Partnerships on record: _____

NOTE: *If the client is a local financial institution or is subject to a licensing regime and regulated by a foreign supervisory body in a country outlined in the First Schedule to the Financial Transactions Reporting Act, Chapter 368 and that supervisory body has AML requirements which are equivalent to or higher than Bahamian standards, the licensee is exempted from providing the information in 12 and 13 below.*

The licensee should note that their clients are required to maintain the relevant information and undertake to provide it to the licensee immediately upon request.

The information in 12 relates to **International Business Companies (IBC's)**.

12. Number/ Percentage of IBCs examined: # %

Please inquire whether the following documents are on file for each IBC examined. Also indicate the number of IBC's examined that have the required information on file and the number of IBC's examined that did not have the required information on file –

Information Required	Number of IBCs <u>with</u> information on file	Number of IBCs <u>without</u> information on file
Instructing client's principal place of business		
Instructing client's business address		
Instructing client's telephone		
Instructing client's facsimile		
Instructing client's electronic address		
Names and addresses of the beneficial owners of the IBC		
Activity that IBC is engaged in		

The information in 13 relates to Exempted Limited Partnerships

13. Number/ Percentage of Exempted Limited Partnerships examined: # %

Please inquire whether the following documents are on file for each Exempted Limited Partnership examined. Also, indicate the number of Exempted Limited Partnerships examined that have the required information on file and the number of Exempted Limited Partnerships examined that did not have the required information on file –

Information Required	Number of Exempted Limited Partnerships <u>with</u> information on file	Number of Exempted Limited Partnerships <u>without</u> information on file
Instructing client's principal place of business		
Instructing client's business address		
Instructing client's telephone		
Instructing client's facsimile		
Instructing client's electronic address		
Names and addresses of the partners in the Exempted Limited Partnership		
Activity that Exempted Limited Partnership is engaged in		

- REMINDER -

IF THE FCSP HAS FACILITIES THROUGH WHICH CLIENTS MAY CONDUCT FINANCIAL TRANSACTIONS, PLEASE COMPLETE SECTION II

IF THE FCSP HAS NO FACILITIES THROUGH WHICH CLIENTS MAY CONDUCT FINANCIAL TRANSACTIONS, SECTION II SHOULD NOT BE COMPLETED.

SECTION II

THE FINANCIAL TRANSACTIONS REPORTING ACT, CHAPTER 368 AND THE ANTI-TERRORISM ACT, 2004

PART III:

RISK-BASED CUSTOMER VERIFICATION PROCEDURES AND RECORDS

Points Scored
(for Commission
use only)

13. Are there policies and procedures that categorize facilities into high or low risk for money laundering showing the criteria used for such categorization?

Yes No

If the answer to Question 13 above is "No", the examiner should not proceed with the examination. The financial institution needs to categorize all facilities into "high" or "low" risk for money laundering.

14. Total number of facilities on record

• Number of high risk facilities

• Number of low risk facilities

15. Total number of facilities examined¹

• Number of high risk facilities

• Number of low risk facilities

16. Has each facility holder for the facilities examined been verified in compliance with the financial institution's policies and procedures for customer verification?

Yes No

13.

16.

¹ The sample of facilities examined should only be taken from financial transactions conducted within the last five years.

		Points Scored (for Commission use only)
<p>17. What number and percentage of facilities examined <u>did not</u> comply with question 16?</p> <p># <input type="text"/> % <input type="text"/></p>	17.	_____
<p>18. Please indicate how many large cash transactions* have been conducted by or for the benefit of a <u>non-facility holder</u> during the current examination period.</p> <p style="text-align: right;"><input type="text"/></p>		
<p>19. What percentage of transactions identified in question 18 were verified in accordance with the financial institution's anti-money laundering policies and procedures?</p> <p style="text-align: right;"><input type="text"/></p>	19.	_____
<p>20. What percentage of transactions identified in question 18 relied upon confirmation letters that verification had been carried out by another financial institution?</p> <p style="text-align: right;"><input type="text"/></p>		
<p>PART IV:</p> <p>TRANSACTIONS RECORD KEEPING PROCEDURES</p>		
<p>21. What is the aggregate number and percentage of the facilities examined that <u>did not</u> have all transaction records as required by Section 23 of the FTRA?</p> <p># <input type="text"/> % <input type="text"/></p>	21.	_____

* A **large cash transaction** refers to any cash transaction of \$15,000 or more.

PART V: SUSPICIOUS TRANSACTIONS REPORTING PROCEDURES		Points Scored (for Commission use only)
<p>22. Name of Money Laundering Reporting Officer (MLRO) _____</p>	22.	_____
<p>23. Has he/she confirmed that he/she is aware of his/her responsibilities under the FI(TR)R Ch. 367?</p> <p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	23.	_____
<p>24. Is the MLRO registered with the FIU? Yes <input type="checkbox"/> No <input type="checkbox"/></p> <p>If "Yes", what is the date of registration? _____</p>	24.	_____
<p>25. Name of Compliance Officer, if different from MLRO? _____</p>		
<p>26. Has the Compliance Officer confirmed that he/she is aware of his/her responsibilities under the FI(TR)R, Ch. 367?</p> <p>Yes <input type="checkbox"/> No <input type="checkbox"/></p>	26.	_____
<p>27. How many suspicious transactions reports have been made to the MLRO during this examination period[§]?</p> <p style="text-align: right;"><input type="text"/></p>		

[§] The examination period should begin at the date of the financial institution's last AML/CFT exam through the date of the current examination.

		Points Scored (for Commission use only)
<p>28. How many suspicious transactions reports have been made to the FIU during this current examination period?</p> <div style="text-align: right; margin-right: 50px;"><input style="width: 50px; height: 20px;" type="text"/></div>		
<p>PART VI: TRAINING AND STAFF AWARENESS PROCEDURES</p>		
<p>29. Is there an AML/CFT staff training programme in place?</p> <p style="margin-left: 40px;">Yes <input style="width: 50px; height: 20px;" type="text"/> No <input style="width: 50px; height: 20px;" type="text"/></p> <p>If "Yes", please attach a copy of the programme.</p>	<p>29.</p> <hr style="width: 100%;"/>	
<p>30. Has any staff participated in AML/CFT training sessions conducted either locally or abroad during the examination period?</p> <p style="margin-left: 40px;">Yes <input style="width: 50px; height: 20px;" type="text"/> No <input style="width: 50px; height: 20px;" type="text"/></p> <p>If "Yes", please attach list of the venue(s), participant(s) and date(s) in Part VI General Comments.</p>	<p>30.</p> <hr style="width: 100%;"/>	
<p>31. Do the FIU 2007 Guidelines and the Compliance Commission's most current Code of Practice form part of the AML/CFT training and awareness procedures for staff?</p> <p style="margin-left: 40px;">Yes <input style="width: 50px; height: 20px;" type="text"/> No <input style="width: 50px; height: 20px;" type="text"/></p>	<p>31.</p> <hr style="width: 100%;"/>	
<p>32. Do internal AML/CFT compliance reviews take place?</p> <p style="margin-left: 40px;">Yes <input style="width: 50px; height: 20px;" type="text"/> No <input style="width: 50px; height: 20px;" type="text"/></p>	<p>32.</p> <hr style="width: 100%;"/>	

DEFINITION TERMS

The terms are defined for the purposes of this Examination as follows:

“**AML**” refers to anti-money laundering

“**Cash**” refers to coins, paper money, travelers’ cheques, postal money orders and other similar bearer type negotiable instruments.

“**CFT**” means combating the financing of terrorism

“**Facility**” refers to any account or arrangement that is provided by a financial & corporate service provider to a client and by, through or with which the client may conduct two or more transactions whether or not they are so used. A facility also specifically includes provision of facilities for safe custody, such as safety deposit boxes.

“**Facility Holder**” refers to the client and any person who is authorized to issue instructions in relation to how transactions should be conducted through a facility, provided by the financial & corporate service provider.

“**Large Cash Transaction**” refers to any cash transaction of \$15,000 or more that is conducted by a facility holder on behalf of another or a non-facility holder; in relation to any facility held by a financial and corporate service provider. An example of this may either be where a facility holder on someone else’s behalf, or a non-facility holder, pays a sum in cash of \$15,000 or more to the financial and corporate service provider to be applied for the benefit of a facility holder.

“**ML/TF**” means Money Laundering and Terrorism Financing

“**FCSP**” refers to a licensed Financial and Corporate Service Provider

“**FCSPA**” refers to the Financial and Corporate Service Providers Act, Ch. 369

“**FTRA**” refers to the Financial Transactions Reporting Act, Ch. 368

“**FTRR**” refers to the Financial Transactions Reporting Regulations, Ch. 368

“**FIU**” refers to the Financial Intelligence Unit.

“**FI(TR)R**” refers to the Financial Intelligence (Transactions Reporting) Regulations Ch. 367

“**Transaction**” refers to any deposit, withdrawal, exchange or transfer of funds in cash, by cheque, payment order or other instrument, and includes electronic transmissions of funds.

THE COMPLIANCE COMMISSION
Inspection Unit

SAMPLING GUIDE

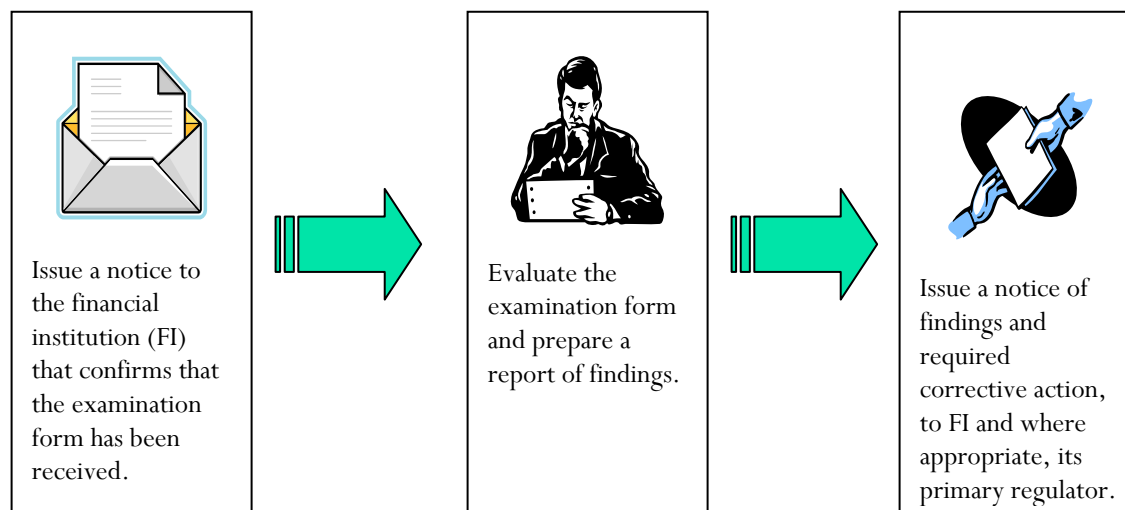
This guide is for the specific use of examiners performing anti-money laundering and combating the financing of terrorism examinations on behalf of the Compliance Commission.

The examiner should use this guide to determine the number of facilities that should be examined during an examination, given the total number of facilities managed by a financial institution.

# OF FACILITIES	PERCENTAGE	MINIMUM/ MAXIMUM NUMBER EXAMINED
1-50	30%	3 / 15
51-100	25%	12 / 25
101-200	20%	20 / 40
201-300	15%	30 / 45
301-500	10%	31 / 50
501-700	6%	35 / 49
701-1,000	6%	42 / 60
1,000-1,500	5%	50 / 75
1,501-2,000	4%	60 / 80
2,001-5,000	2%	40/100
5,001-10,000	1%	50/100
10,001-25,000	.5%	50/125
>25,000	.25%	*

COMPLIANCE COMMISSION
EVALUATION PROCESS FOR EXAMINATIONS

When an accountant has completed an examination of a financial institution, the accountant is required to submit the examination form to the Compliance Commission (the Commission). The Commission will then:



After an AML/CFT examination form is completed, the Commission’s Examiners evaluate the financial institution’s level of compliance by assigning a score to specific questions on the form. F.I.’s that score points of 95% to 100% are given a rating of “Good” while F.I.’s that score less than 80% are given a rating of “Very Poor”. The table below illustrates the rating system for examinations.

Rating System for Examinations

Rating	Good	Acceptable	Poor	Very Poor
% Points	95% -100%	90%-94%	80%-89%	Less than 80%

Examinations which are rated ‘Poor’ or ‘Very Poor’ reveal that a financial institution is not in compliance with AML/CFT laws. Poorly rated financial institutions are informed about their specific deficiencies and a follow-up examination is arranged to address the weak areas.

During a follow-up examination, the financial institution is given advice on corrective action that must be taken to bring the institution in full compliance with AML/CFT laws. The entire follow-up process is completed after all plans for corrective action are discussed and executed by the financial institution.

Money Laundering /Terrorist Financing Offences, Penalties and Defences

Money Laundering Offences

The POCA establishes several specific money laundering offences and penalties in performing their functions, FCSPs should pay particular attention to the vulnerabilities of their service inherent in these offences.

N.B. THE OFFENCES UNDER THE POCA APPLY TO ALL PERSONS AND ARE NOT LIMITED ONLY TO THOSE CIRCUMSTANCES WHERE A FCSP IS ACTING AS A FINANCIAL INSTITUTION. THEY ARE THEREFORE APPLICABLE TO RELEVANT CIRCUMSTANCES AFFECTING ALL SERVICES PROVIDED BY THE FCSP UNLIKE THE FTRA WHICH IS RESTRICTED TO THOSE CIRCUMSTANCES IN WHICH A FCSP IS ACTING AS A FINANCIAL INSTITUTION.

In addition, there are many offences which arise from failing to comply with certain requests or obligations imposed under the FTRA, the Financial Intelligence Unit Act and the Regulations made pursuant to these Acts. A matrix of these offences also appears hereunder.

(1) MONEY LAUNDERING OFFENCES, PENALTIES AND DEFENCES UNDER THE PROCEED OF CRIME ACT, CH. 93

For the purposes of the POCA, the term “criminal conduct” includes (1) drug trafficking, (2) bribery and corruption, (3) money-laundering, (4) any offence which may be tried in the Supreme Court of The Bahamas other than a drug trafficking offence and (5) an offence committed anywhere that, if committed in The Bahamas, would constitute an offence in The Bahamas as set out in the Schedule to the Proceed of Crime Act, Ch. 93.

The term “property” is defined under the POCA to mean, money and all other property, moveable or immovable, including things in action and other intangible and incorporeal property.

<i>Offence</i>	<i>Penalties</i>	<i>Defences</i>
<p><u>Concealing, Transferring Or Dealing With The Proceeds Of Criminal Conduct (Section 40)</u></p> <p>It is an offence to use, transfer, send or deliver to any person or place, or to dispose of or otherwise deal with any property, for the purpose of concealing or disguising such property, knowing, suspecting or having a reasonable suspicion that the property (in whole or in part, directly or indirectly) is the proceeds of criminal conduct. For this offence references to concealing or disguising property includes concealing or disguising the nature, source, location, disposition, movement or ownership or any rights with respect to the property. This section applies to a person’s own proceeds of criminal conduct or where he knows or has reasonable grounds to suspect that the property he is dealing with represents the proceeds of another’s criminal conduct.</p>	<p>On summary conviction - 5 years imprisonment or a fine of \$100,000, or both.</p> <p>On conviction on information - imprisonment for 20 years or to an unlimited fine or both.</p>	
<p><u>Assisting Another To Conceal The Proceeds Of Criminal Conduct (Section 41).</u></p> <p>It is an offence for any person to provide assistance to a criminal for the purpose of obtaining, concealing, retaining or investing funds, <u>knowing</u> or suspecting, or having reasonable grounds to suspect that those funds are the proceeds of serious criminal conduct and/ or a “relevant criminal offence”.</p>	<p>On summary conviction - 5 years imprisonment or a fine of \$100,000, or both.</p> <p>On conviction on information to imprisonment for 20 years or to an unlimited fine or both. <i>It is important to note that these are mandatory penalties.</i></p>	<p>It is a defence that the person concerned did not know, suspect or have reasonable grounds to suspect that the funds in question are the proceeds of serious criminal conduct, or that he intended to disclose to a police officer his suspicion, belief or any matter on which such suspicion or belief is based, but there is a reasonable excuse for his failure to make a disclosure.</p>

Offence	Penalties	Defences
<p><u>Acquisition, Possession Or Use (Section 42)</u></p> <p>It is an offence to acquire, use or possess property which are the proceeds (whether wholly or partially, directly or indirectly) of criminal conduct, knowing, suspecting or having reasonable grounds to suspect that such property are the proceeds of criminal conduct. Having possession is construed to include doing any act in relation to the property.</p>	<p>On summary conviction by 5 years imprisonment or a fine of \$100,000, or both.</p> <p>On conviction on information to imprisonment for 20 years or to an unlimited fine or both. <i>(It is important to note that these are mandatory penalties).</i></p>	<p>That the property in question was obtained for adequate consideration. [NB: The provisions of goods or services which assist in the criminal conduct does not qualify as consideration for the purposes of this offence.]</p>
<p><u>Failure To Disclose (Section 43)</u></p> <p>It is an offence if a person fails to disclose to the FIU or a police officer that another person is engaged in money laundering related to proceeds of drug trafficking or a relevant offence where he knows, suspects or has reasonable grounds to suspect that such is the case and that knowledge or suspicion came to his attention in the course of his trade, profession, business or employment. Disclosure to the MLRO will suffice as disclosure to the authorities under this section.</p>	<p>On summary conviction - 5 years imprisonment or a fine of \$100,000, or both;</p> <p>On conviction on information - imprisonment for 20 years or to an unlimited fine or both.</p>	<p>It is a defence to prove that the defendant took all reasonable steps to ensure that he complied with the statutory requirement to report a transaction or proposed transaction to the Financial Intelligence Unit; or that in the circumstances of the particular case, he could not reasonably have been expected to comply with the provision.</p>
<p><u>Tipping Off (Section 44)</u></p> <p>It is also an offence for anyone who knows suspects or has reasonable grounds to suspect that a disclosure has been made, or that the authorities are acting, or are proposing to act, in connection with an investigation into money laundering, to prejudice an investigation by so informing the person who is the subject of a suspicion, or any third party of the disclosure, action or proposed action. Preliminary enquiries of a customer in order to verify his identity or to ascertain the source of funds or the precise nature of the transaction being undertaken will not trigger a tipping off offence before a suspicious transaction report has been submitted in respect of that customer <u>unless</u> the enquirer knows that an investigation is underway or the enquiries are likely to prejudice an investigation.</p> <p>Where it is known or suspected that a suspicious transaction report has already been disclosed to the Financial Intelligence Unit, the Police or other authorised agencies and it becomes necessary to make further enquiries, great care should be taken to ensure that customers do not become aware that their names have been brought to the attention of the authorities.</p>	<p>The punishment on summary conviction for the offence of "tipping-off" is a term of three years imprisonment or a fine of \$50,000, or both;</p> <p>On conviction on information the penalty is a term of imprisonment for ten years or an unlimited fine or both (see sections 44 and 45 of the Proceed of Crime Act, 2000 Ch. 93).</p>	<p>It is a defence if the person making the disclosure did not know or suspect that the disclosure was likely to prejudice the investigation, or that the disclosure was made under a lawful authority or with reasonable excuse.</p>

(2) MONEY LAUNDERING RELATED OFFENCES UNDER THE FTRA & FI(TR)R

These offences relate to the various AML obligations imposed on financial institutions.

Offence	Penalties	Defences
<u>Failing or refusing to provide records, information or explanation when required to do so by the Commission (FTRA)</u>	Maximum fine on summary conviction is \$50,000 or 3 years imprisonment or both.	
<u>Verification Offences (FTRA s. 12)</u> It is an offence in each case to proceed to allow for the provision of a new facility or the conduct of any occasional transaction as the case may be without having verified the identity of the customer and any person on whose behalf he may be acting as required.	On summary conviction: Maximum fine of \$20,000 for individuals and \$100,000 for Corporations.	<i>Either</i> that all reasonable steps were taken to verify or under the circumstances could not reasonably be expected to ensure that verification has been satisfied. ²⁵
<u>Recordkeeping Offences (FTRA s. 30)</u> Failure to maintain records as required.	On summary conviction \$20,000 maximum in the case of an individual and \$100,000 maximum in the case of a corporation.	
<u>Suspicious Transactions Reporting Offences (FTRA s. 20)</u> (1) Failure to make an STR in circumstances that would require that a report be made. (2) Knowingly making any statement that is false or misleading in a material particular; or knowingly omitting from any statement any matter or thing without which the statement is false or misleading in a material particular. (3) Disclosing information about the contemplation or existence of an STR - (a) for the purpose of obtaining, directly or indirectly, an advantage or a pecuniary gain for yourself or any other person; or (b) intentionally to prejudice any investigation into the commission or possible commission of a money laundering offence. (4) Disclosing information about the contemplation or existence of an STR.	On summary conviction a \$20,000 max. fine for an individual and \$100,000 for a corporation. On summary conviction a maximum fine of \$15,000. Maximum penalty on summary conviction: 2 years imprisonment. On summary conviction a maximum fine of \$5,000 or 6 months imprisonment for an individual and in the case of a corporation a maximum fine of \$20,000.	Same as the defence for failing to verify.
<u>Failure to comply with any regulation under the Financial Intelligence (Transactions Reporting) Regulations or comply with any guideline, code of practice, directive, rules or other instructions issued by the FIU or a Regulator</u> e.g. Maintain Internal Reporting Procedures, appoint an MLRO, provide staff education and training programmes in the detection and prevention of money laundering.	Punishable by a fine of \$10,000 on summary conviction or \$50,000 for a first offence, and \$100,000 for any subsequent offence on conviction in the Supreme Court.	It is a defence to for the financial institution to prove that it took all reasonable steps and exercised due diligence to comply with the requirements of the regulations, guidelines, codes or instructions as the case may be

²⁵ Notice of Defence must be served on the prosecution within 21 days of the summons being served, with particulars of the defence. The court is empowered to grant an extension of time for the service of the notice.

(3) (a) TERRORIST FINANCING OFFENCES UNDER THE ANTI-TERRORISM ACT

<i>Offence</i>	<i>Penalties</i>	<i>Defences</i>
<p><u>Offence of Terrorism (s. 3)</u> The carrying out (or aiding, abetting, counseling, procuring, inciting, conspiring or soliciting the carrying out) of an act: (a) that constitutes an offence under in any of the Treaties listed in the First Schedule; or (b) for the purpose of intimidating the public or compelling a government/international organization to do or to refrain from doing anything that is intended to cause -</p> <ol style="list-style-type: none"> death or serious bodily harm to a civilian; serious risk to health or safety of the public; substantial property damage; ; or serious interference with an essential service, facility or system. 	<p>On conviction on information where death ensues, murder or treason, the maximum sentence is death. In other cases the maximum penalty is life imprisonment.</p>	
<p><u>Providing or collecting funds for criminal purposes. (s.5)</u> Providing or collecting funds; or providing financial services or making such services available to persons, whether by means that are direct or indirect, unlawful and willful (including through aiding, abetting, counseling, procuring, inciting, conspiring or soliciting in relation thereto) with the intention that the funds or services are to be used or with the knowledge that the funds or services are to be used in full or in part in order to carry out an offence of terrorism under section 3.</p>	<p>On conviction on information, a maximum imprisonment term of 25 years.</p>	
<p><u>Liability of a legal entity (Anti-Terrorism Act 2004 s.6)</u></p> <p>Where an offence referred to under sections 3 or 5 is committed by a person responsible for the management or control of an entity located or registered in The Bahamas or in any other way organized under the laws of The Bahamas, that entity is also liable, in circumstances where the person committed the offence while in that capacity.</p>	<p>Maximum penalty on conviction – two million dollars (\$2M).</p>	
<p><u>Duty to Report (s.7)</u> Failure to report, where there are reasonable grounds to suspect that funds or financial services are related to or are to be used to facilitate an offence under the Act.</p>	<p>On conviction on information a maximum penalty of a fine of \$250,000 or to imprisonment for a term of 5 years.</p>	

The ATA incorporates all offences contained in the Treaties listed in its First Schedule, which are reproduced in 3 (b) below. It is important to note that terrorist offences in the ATA have been incorporated into the list of predicate offences appearing in the First Schedule of POCA and thereby subject to the requirement imposed upon FCSPs under the FTRA and the FIUA. Section 7 of the ATA requires the reporting of offences under the Act to be made to the Commissioner of Police.

(3) (b) THE FIRST SCHEDULE TO THE ATA - LIST OF TREATIES RELATIVE TO TERRORISM

- Convention on offences and certain other acts committed on Board Aircraft signed at Tokyo 14th September, 1963.
- Convention for the Suppression of Unlawful Seizure of Aircraft, done at the Hague on 16th December, 1970.
- Convention for the Succession of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 13th September, 1971.
- Convention on the Prevention and Punishment of Crimes against Internationally protected persons including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14th December, 1973.
- International Convention against the taking of Hostages, adopted by the General Assembly of the United Nations 17th December, 1979.
- International Convention for the Suppression of the Financing of adopted by the General Assembly of the United Nations on 9th December, 1999.
- Inter-American Convention Against Terrorism adopted at the Second Plenary Session of the Organization of American States held June 3, 2002.
- Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on 10th March 1988.
- Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, done at Rome on 10th March 1988.
- International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15th December, 1997.
- Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed at Montreal on 24th February, 1988.
- Convention on the Marking of Plastic Explosives for the Purpose of Detection signed at Montreal on 1st March, 1991.
- Convention on the Physical Protection of Nuclear Material signed at Vienna on 3rd March 1980.

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

Dear Sirs:

REQUEST FOR VERIFICATION OF CUSTOMER IDENTITY

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

Full name of customer

Title (MR/MRS/MISS/MS) SPECIFY

Address including postcode
(as given by customer)

Date of birth Account Number
(if known)

Example of customer's signature

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

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

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

With reference to your enquiry dated we:

- 1) Confirm that the above customer *is/is not known to us.
- 2) *Confirm/cannot confirm the address shown in your enquiry.
- 3) *Confirm/cannot confirm that the signature reproduced in your enquiry appears to be that of the above customer.

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

*Delete as applicable.

[C] Subject(s) of Disclosure - Company

Company Name:.....

Type of Business:.....

Full Address:

.....

Telephone No.: Fax No.:

E-mail Address:

Identification Documents (e.g., certificate of incorporation, memorandum and articles of association, etc. *if available*):

.....

[D] Beneficial Owner(s)

(of the assets being the subject(s) of disclosure – if different from the subject(s) of disclosure above)

Full Name:

Date and Place of Birth (Individual):.....

Type of Business/Occupation:

Full Address:

.....

.....

.....

Telephone No. (Work): Telephone No. (Home):

Fax: E-mail Address:

[E] Authorised Signatories

*Information on authorised signatories and/or persons with power of attorney.
(List further persons in an annex in the same manner as required below)*

Full Name (Individual):.....

Date and Place of Birth (Individual):.....

Occupation:.....

Full Address:

.....

.....

Telephone No. (Work): Telephone No. (Home):

Fax: E-mail Address:

STATISTICAL INFORMATION

Nature of Institution	Please tick	Grounds for Disclosure? <i>Please tick all that apply</i>	Please tick
Bank		Media / Publicity	
Fund Managers		Internet Research	
Bureaux Des Changes		Group Information	
Stockbrokers		3 rd Party Information	
Financial Advisors		Service of Production, Charging or Monitoring Order	
Insurance Companies		Police enquiry	
Trust Company		Account Activity Not in Keeping with KYC	
Corporate Service Provider		Evidence of Forged Documentation	
Lawyers		Cash Transactions	
Accountants		Transitory Accounts – Immediate Layering	
Local Regulator		High Risk Jurisdictions	
Other Regulator		Unusual Forex Transactions	
Other (specify)		Purchase and Surrender of Insurance Policy	
		Repeat disclosures	
Trends?		Failure to comply with due diligence/checks	
Involving at least one intermediary		Other (specify)	
Long Standing Customer			
New Customer			
Electronic Banking		What currency was involved?	
EURO Transaction		GBP	
		USD	
		EUR	
Criminality Suspected		ESP	
Drugs		GDM	
Terrorism		ITL	
Fraud		FRF	
Revenue Fraud		IEP	
Insider Dealing		SEK	
Corruption		CHF	
Unknown / undetermined		BSD	
Regulatory Matters		OTHER	
Other			

Completed forms should be forwarded to the Financial Intelligence Unit,
3rd Floor, Norfolk House, Frederick Street, P.O. Box SB-50086, Nassau, The Bahamas.
Telephone No: (242) 356-9808 or (242) 356-6327, Fax No. (242) 322-5551

FINANCIAL AND CORPORATE SERVICE PROVIDERS - TYPOLOGIES

Source: FATF Money Laundering Typology Reports 2006

Case 1: Use of Multi-jurisdictional structures of corporate entities and trusts

Mr. [A] was a trust service provider operating a trust company [L]. Using a series of domestic trusts that he established, he wired large sums of money to 51 different US and offshore bank accounts. In total it is estimated the scheme defrauded over 500 investors of approximately \$56 million.

The thrust of the scheme was that A and associates convinced their clients to form [“Pure Trust Organizations”(PTO)] and to place their life savings, including their retirement accounts, into these trusts created by [L]. Clients were advised that the [PTO] provided asset protection providing concealment of their assets from the government and other creditors. The [L] package promised the formation of a [PTO] and off- shore bank accounts. The clients were told that when the funds were placed in these off-shore bank accounts the funds was beyond the reach of the US government and any creditor.

Once the clients had placed their assets into the trusts, [A] used another corporation to provide investments for the assets in the trusts. In reality there were no real investments, and [A] and his associates defrauded the trust owners.

Case 7: Use of Nominees

Mr [B] and his associate bought insurance companies. The assets of these companies were drained and used for personal benefits. The draining of the assets was concealed by transferring them into accounts in and out the US via wire transfers. The first step in the scheme was establishing a trust in the US. [B] concealed his involvement and the control of the trust through the use of nominees as grantors and trustee. [B] then used the trust to purchase the insurance companies. Immediately after the acquisition, [B] would transfer millions of dollars of reserve assets to a corporation he set up in the US. The funds were then wire-transferred to an offshore bank account in the name of another corporation that he controlled. Once these funds were deposited into the offshore bank account, [B] used them to pay for his personal expenses.

Source: FATF Terrorism Financing Typology Report 2004

Case 2: Terrorist organisation uses wire transfers to move money across borders.

A terrorist organisation in Country X was observed using bank wire transfers to move money in Country Y that was eventually used for paying rent for safe houses, buying and selling vehicles, and purchasing electronic components with which to construct explosive devices. The organisation used “bridge” or “conduit” accounts in Country X as a means of moving funds between countries. The accounts at both ends were opened in the names of people with no apparent association with the structure of terrorist organisation but who were linked to one another by kinship or similar ties. There were thus the apparent family connections that could provide a justification for the transfers between them if necessary.

Funds, mainly in the form of cash deposits by the terrorist organisation were deposited into bank accounts from which the transfers are made. Once the money was received at the destination, the holder either left it on deposit or invested it in mutual funds where it remained hidden and available for the organisation’s future needs. Alternatively, the money was transferred to other bank accounts managed by the organisation’s correspondent financial manager, from where it was distributed to pay for the purchase of equipment and material or to cover other ad hoc expenses incurred by the organisation in its clandestine activities.