SAINT VINCENT AND THE GRENADINES

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING CODE 2017

ARRANGEMENT OF PARAGRAPHS

Paragraph

SAINT VINCENT AND THE GRENADINES

STATUTORY RULES AND ORDERS

2017 NO. 24

(Gazetted 9th May, 2017)

IN EXERCISE of the powers conferred by section 169 of the Proceeds of Crime Act 2013, No 38 of 2013, the National Anti-Money Laundering Committee issues the following Code:

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING CODE, 2017

PART 1

PRELIMINARY, SCOPE AND INTERPRETATION

Citation and commencement

1. This Code may be cited as the Anti-Money Laundering and Terrorist Financing Code, 2017 and comes into force on the day the 2017 amendment to Proceeds of Crime Act 2013 comes into force.

Scope of Code

2. This Code applies to all service providers, Non-Regulated Service Providers and, to the extent specified, to boards and directors of service providers.

Interpretation

3. (1) In this Code:

"Act" means the Proceeds of Crime Act, 2013;

"Authority" means the Saint Vincent and the Grenadines Financial Services Authority, established by the Financial Services Authority Act 2011;

"board" means:

(a) in relation to a legal person, the board of directors, committee of management or other governing

authority of the company, by whatever name called or, if the company only has one director, that director;

(b) in relation to a foundation, the Foundation Council or other governing authority of the foundation, by whatever name called;

(c) in relation to a partnership, the partners, or in the case of a limited partnership, the general partners; or

(d) in relation to any other legal person, the persons fulfilling functions equivalent to the functions of the directors of a company;

"Committee" means the National Anti-Money Laundering Committee established under section 118 of the Act;

"customer risk assessment" means the risk assessment carried out in accordance with regulation 13(2)(b) of the Regulations;

"minimum retention period: in relation to records, shall be construed in accordance with paragraph 3;

"Regulations" means the Anti-Money Laundering and Terrorist Financing Regulations 2014.

(2) Unless the context otherwise requires, any word or phrase defined in the Act or in the Regulations has the same meaning in this Code.

GUIDANCE NOTES

Introduction

(i) In common with all countries, both offshore and on-shore, St Vincent and the Grenadines has a responsibility to comply with international standards concerning the prevention and detection of money laundering and the combating of terrorist financing. These standards are set primarily by the Financial Action Task Force ("the FATF"). The current FATF standards are known as the "FATF Recommendations", which cover the prevention and

detection of money laundering and the combating of terrorist financing. However, the Basel Committee on Banking Supervision, the International Organization of Securities Commissions and the International Association of Insurance Supervisors also set sector specific anti-money laundering standards for banking, securities and investment business and insurance business respectively. In addition, St Vincent and the Grenadines is a member of the Caribbean Financial Action Task Force, a grouping of Caribbean states that have agreed to implement common counter measures to address money laundering and terrorist financing.

(ii) St Vincent and the Grenadines is committed to complying with its international obligations and to keeping the country's anti-money laundering and terrorist financing legislation up to date. Following a thorough review, new Proceeds of Crime Act ("the Act") was enacted in December 2013 and came into force on April 9, 2014. The Act repealed the Proceeds of Crime (Money Laundering and Prevention) Act and certain provisions of the Drug Trafficking Offences Act. The Act is supported by the Proceeds of Crime (Anti-Money Laundering and Terrorist Financing) Regulations 2014 ("the Regulations") and the Proceeds of Crime (Anti-Money Laundering and Terrorist Financing) Code 2017 ("the Code").

(iii) In summary, the Act is designed to:

(a) criminalise money laundering;

(b) provide for the confiscation of the proceeds of criminal conduct;

(c) enable the civil recovery of property which represents, or is obtained through, unlawful conduct;

(d) require persons in the financial sector to report knowledge or suspicions concerning money laundering to the FIU;

(e) give the High Court the power to make a number of orders to assist the police in their investigations into money laundering;

(f) continue the Confiscated Assets Fund; and

(g) provide for the issuance of the Regulations and the Code to enable the establishment of a framework for the prevention and detection of money laundering and terrorist financing.

(iv) The Act does not provide for the combating of terrorist financing. This is covered by the Anti-Terrorist Financing and Proliferation Act 2015, No. 14 of 2015.

(v) Service providers in St Vincent and the Grenadines are one of the most important lines of defence against the use of the jurisdiction for money laundering and terrorist financing. The Regulations therefore impose requirements on service providers with respect to measures to be taken by them to prevent money laundering and terrorist financing. Most breaches of the Regulations constitute an offence. The Regulations are supplemented by the Code.

(vi) The obligations contained in the Act, the Regulations and the Code will be rigorously enforced. However, it is in the interests of St Vincent and the Grenadines as a jurisdiction that efforts to prevent money laundering and terrorist financing are undertaken in a spirit of cooperation between the public and private sectors. Furthermore, regardless of the legal obligations imposed on them by the Act, the Regulations and the Code, it is very much in the interests of all service providers to have strong systems in place to reduce the risk that they are used in connection with money laundering or terrorist financing. The use of a service provider in St Vincent and the Grenadines in connection with money laundering or terrorist financing is likely to damage the reputation of the business and of the jurisdiction as a financial services centre, which could lead to a loss of legitimate business. It is therefore important that every service provider understand the important role it plays in protecting the reputation of the jurisdiction. Furthermore, a service provider that assists in the laundering of money or terrorist financing risks possible prosecution for a money laundering or terrorist financing offence, enforcement action, administrative penalties and, if a regulated person, the loss of its licence. Breaches of the Act, the Regulations and the Code could also result in the directors of a service provider being prosecuted for a criminal offence.

(vii) A service provider is best able to protect itself from being used in connection with money laundering or terrorist financing by maintaining effective procedures, systems and controls, including sound customer due diligence procedures, that comply with international standards, and rigorously implementing them. The Regulations and the Code set out requirements imposed on service providers for the prevention of money laundering and the combating of terrorist financing that supplement the requirements of the Act and the Regulations. The Committee considers that the legal regime taken as a whole enables St Vincent and the Grenadines to meet international standards.

Purpose of the Code

(viii) The purpose of the Code is to:

(a) sepsed for money laundering or terrorist financing.

It is therefore essential that all persons to whom the Code applies adopt an intelligent risk-sensitive approach and establish and maintain systems and procedures that are appropriate and proportionate to the risks identified.

Status of Code

(x) The Code has been issued by the Committee under section 169 of the Act. The Act provides that the Code is subordinate legislation and has full legislative effect. In the circumstances, the Code has the status of "law" in St Vincent and the Grenadines.

(xi) The Code:

(a) must be complied with by every person to whom it applies;

(b) has effect as law and therefore has the same legal force as if the provisions in the Code had been contained in the Act or the Regulations; and

(c) is enforceable against a service provider by its supervisory authority.

Breaches of the Code may attract a penalty and, in certain circumstances, constitute an offence.

(xii) Although the Code has full effect on the date specified in the Code, the House of Assembly may, by resolution, annul the Code or an amendment to the Code [section 169(7)].

Status of Guidance Notes

(xiii) The Guidance Notes has been issued by the Committee under section 169(9) of the Act. The purpose of the Guidance Notes is to:

(a) outline the relevant requirements of the Act, the Regulations, the Code, the terrorist financing law and other relevant legislation with respect to the prevention of money laundering and terrorist financing;

(b) provide guidance to assist service providers to interpret the requirements of the Act, the Regulations and the Code;

(c) provide important background or Guidance information;

(d) provide practical guidance on identification and verification of identity;

(e) set out the factors that a supervisory authority will take into account in considering whether or not a requirement in the Act, the Regulations or the Code has been complied with; and

(f) provide guidance on how the Committee expects service providers to comply with the Regulations and the Code.

(xiv) Although the Guidance Notes do not have the status of "law", section 168(4) of the Act requires the Court to consider whether a person has followed any guidance issued by the Committee in deciding whether a person has committed an offence under the Regulations. A supervisory authority will also consider whether the Guidance Notes have been followed in deciding whether a service provider has failed to comply with the Code.

(xv) In order to assist in explaining the AML/CFT framework, the Guidance Notes paraphrases some of the requirements of the Act, the Regulations and the Code. However, the original text of each is the authoritative source and should always be referred to in interpreting the various provisions and requirements.

The Guidance Notes cannot, of course, modify or in any way dilute the requirements of the Regulations or the Code. If there is any

inconsistency between the Guidance Notes and the Regulations or Code, the Regulations or the Code prevail.

(xvi) Although the Committee expects senior management of service providers to use the Code and the Guidance Notes in the design of service providers' policies, procedures, systems and controls and in the preparation of service providers' procedures manuals, the Code and Guidance Notes are not suitable for adopting by a service provider as its own procedures manual as these must be tailored to the individual requirements of a service provider.

Scope of the Code

(xvii) The Code applies, to the extent specified, to all service providers and their boards and directors. A "service provider" is a person specified as a service provider in Schedule 1 of the Regulations.

There are 3 types of service providers:

(a) regulated persons, that is persons regulated by the Authority;

(b) externally regulated persons, that is persons regulated by the Eastern Caribbean Central Bank or the Eastern Caribbean Securities Regulatory Commission; and

(c) non-regulated service providers, that is certain non-financial businesses and professions whose businesses are considered to pose a money laundering or terrorist financing risk to the jurisdiction. These non-financial businesses and professions, which are termed "non-regulated service providers", include real estate agents, lawyers and accountants regulated by the Financial Intelligence Unit.

car dealers Jewellers

(xviii) The Code applies to all non-regulated service providers unless expressly stated otherwise in the Code. It should be noted that service providers may include any form of legal person, including partnerships, and individuals.

Application of Regulations and Code outside St Vincent and the Grenadines

(xix) Regulation 2 of the Regulations provides that the Regulations and the Code apply to an overseas branch (which includes a representative or contact office) or subsidiary of a relevant service provider (as defined in the Regulations), to the extent that the

laws of the foreign country permit. This is designed to ensure that service providers in St Vincent and the Grenadines apply standards equivalent to the FATF Recommendations throughout their financial services business, wherever the business is situated or carried on.

(xx) Where the laws of the foreign country do not permit this, the service provider's supervisory authority must be informed in writing and, to the extent that the laws of the foreign country permit, the service provider must apply alternative measures to ensure compliance with the FATF Recommendations and to deal effectively with the risk of money laundering and terrorist financing.

Enforcement of the Code

(xxxi)The Regulations and the Code are enforceable:

(a) against regulated persons, by the Financial Services Authority;

(b) against non-regulated service providers, by the Financial Intelligence Unit;

(c) against externally regulated service providers who hold a licence granted under the Banking Act, by the Eastern Caribbean Central Bank;

(c) against externally regulated service providers who hold a licence granted under the Securities Act, by the Eastern Caribbean Securities Regulatory Commission.

(xxii)Each of the above supervisory authorities is empowered to take enforcement action if the service provider has contravened or is in contravention of the Regulations or the Code and the Act provides supervisory authorities with a range of enforcement powers, including the power to impose financial penalties. In the case of a regulated person, non-compliance with the Regulations or the Code will also be taken into account by the Authority in assessing whether a regulated person is "fit and proper" to hold a regulatory licence.

(xxiii)Compliance by service providers with their AML/CFT obligations will form part of supervisory authorities' assessment of service providers when undertaking on-site compliance visits.

It will also form part of supervisory authorities' on-going monitoring of service providers.

Definitions ["company" and "legal person"]

(xxiv)The term "company" is defined in the Act as "a body corporate, wherever incorporated, registered or formed", and includes a foundation. The term therefore covers all types of corporate body. The term "legal person", however, includes partnerships, whether limited or general and any other type of association or unincorporated body of persons, except for trusts.

PART 2

CUSTOMER DUE DILIGENCE MEASURES

Customer due diligence measures to be applied by service provider

4. (1) The customer due diligence information that a service provider is required to obtain under the Regulations shall comprise:

(a) identification information in accordance with paragraph 8, 10, 13 or 15 of this Code as the case may be; and

(b) relationship information in accordance with paragraph 5 of this Code;

(2) A service provider shall:

(a) consider, on a risk-sensitive basis, whether further identification or relationship information is required; and

(b) verify the identity of the customer and any third party and take reasonable measures, on a risk-sensitive basis, to verify the identity of each beneficial owner of a customer or third party in accordance with regulation 6(1)(e) of the Regulations and the relevant paragraphs of this Code.

Relationship information

5. (1) The relationship information obtained by a service provider shall include information concerning:

(a) the purpose and intended nature of the business relationship;

(b) the type, volume and value of the expected activity;

(c) the source of funds and, where the customer risk assessment indicates that the customer, business relationship or occasional transaction presents a high risk, the source of wealth of the customer, third party or beneficial owner;

(d) details of any existing relationships with the service provider;

(e) unless the customer is resident in the State, the reason for using a service provider based in the State; and

(f) such other information concerning the relationship that, on a risk-sensitive basis, the service provider considers appropriate.

(2) Where the customer, third party or beneficial owner is the trustee of a trust or a legal person (including a company), a service provider shall obtain the following relationship information:

(a) the type of trust or legal person;

(b) the nature of the activities of the trust or legal person and the place or places where the activities are carried out;

(c) in the case of a trust:

(i) where the trust is part of a more complex structure, details of that structure, including any underlying companies or other legal persons, and

(ii) classes of beneficiaries or charitable objects;

(d) in the case of a legal person, its ownership and, where the legal person is a company, details of any group of which the company forms a part, including details of the ownership of the group;

(e) whether the trust, the trustee(s) or the legal person is subject to supervision in or outside the State and, if so, details of the relevant supervisory body.

GUIDANCE NOTES

Introduction

(i) The maintenance and operation by the financial services sector of adequate customer due diligence measures is fundamental to the efforts of St. Vincent and the Grenadines to combat money laundering and terrorist financing.

(ii) A service provider must carry out adequate customer due diligence for the following reasons:

(a) customer due diligence helps to protect a service provider, and the jurisdiction, from the risk of being used as a vehicle for money laundering, terrorist financing or other financial crime, helps to protect the service provider from becoming a victim of financial crime and helps to protect against identity fraud;

(b) a service provider that has carried out customer due diligence is able to assist law enforcement agencies by providing information on customers and potential customers and on activities or transactions that are subject to investigation; and

(c) customer due diligence has an essential role to play in a service provider's own risk management procedures.

(iii) Customer due diligence information will also assist a service provider, and its AML/CFT reporting officer and employees, to assess whether a suspicious activity report should be made.

What is "customer due diligence"?

(iv) The term "customer due diligence measures" is defined in regulation 6 of the Regulations. In essence, effective customer due diligence measures will require a service provider to carry out a number of steps for:

(a) identifying who a customer is and whose identity needs to be verified;

(b) verifying the identity of the customer using documents, data or information obtained from a reliable and independent source;

(c) determining whether the customer is acting for a third party and, if so, identifying the third party;

(d) where the customer (or any third party) is not an individual acting in his or her own right, identifying the beneficial owners of the customer or third party, or in the case of a foundation, the persons concerned with the foundation;

(e) verifying the identity of any third parties and of the beneficial owners of the customer and any third parties;

(f) understanding the circumstances and business of a customer, including where appropriate the source of wealth and funds, the purpose of the business relationship with the service provider and the expected nature and level of transactions;

(g) keeping the information held up to date and valid;

(h) the ongoing monitoring of transactions undertaken and the business relationship with the purpose of assessing the extent to which the transactions and activity carried on by the customer are consistent with his circumstances and business and the intended business relationship.

(v) It should be noted that the Regulations include within the definition of beneficial owner, an individual who exercises ultimate control over the management of a legal person, partnership or arrangement, whether alone or jointly [regulation 4(1)(b)].

Summary of principal requirements of Regulations with respect to customer due diligence

(vi) Regulation 11(1) of the Regulations imposes a requirement on service providers to apply customer due diligence measures:

(a) before establishing a business relationship with a customer or carrying out an occasional transaction;

(b) where the service provider suspects money laundering or terrorist financing or doubts the veracity or adequacy of documents, data or information previously obtained under its due diligence measures or when conducting on-going monitoring; and

(c) at other appropriate times to existing customers as determined on a risk-sensitive basis.

(vii) Regulation 13(1) of the Regulations includes a requirement to establish, maintain and implement appropriate risk-sensitive policies and procedures relating to customer due diligence measures and on-going monitoring.

(viii) Regulation 20(2) of the Regulations requires that the policies and procedures, including those relating to customer due diligence measures, must include policies and procedures which provide for:

(a) the identification and scrutiny of:

(I) complex or unusually large transactions;

(II) unusual patterns of transactions which have no apparent economic or visible lawful purpose; and

(III) any other activity which the service provider regards as particularly likely by its nature to be related to the risk of money laundering or terrorist financing;

(b) the taking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products and transactions which are susceptible to anonymity;

(c) determining whether:

(I) a customer, any third party for whom the customer is acting and any beneficial owner of the customer or third party, is a politically exposed person;

(II) a business relationship or transaction, or proposed business relationship or transaction, is with a person connected with a country that does not apply, or insufficiently applies, the FATF Recommendations;

(III) a business relationship or transaction, or proposed business relationship or transaction, is with a person connected with a country or territory that is subject to measures for purposes connected with the prevention and detection of money laundering or terrorist financing,

imposed by one or more countries or sanctioned by the European Union or the United Nations.

(ix) Regulation 14 of the Regulations sets out the circumstances in which a service provider must, on a risk-sensitive basis, apply enhanced customer due diligence measures.

Risk-sensitive approach to due diligence measures

(x) The Regulations and the Code require a service provider to apply a risk-sensitive approach to its customer due diligence measures. The advantages and features of a risk-sensitive approach are covered generally in the Guidance Notes to Part 3 of the Code and this Guidance Notes should be read together with that Guidance Notes. *However, it should, of course, be appreciated that the minimum requirements of the Regulations and the Code must at all times be complied with.*

(xi) Paragraph 2 of the Code requires a service provider to carry out a risk assessment. The risk assessment will enable the service provider to determine its initial approach to designing appropriate customer due diligence procedures for different types of customer. A risk-sensitive approach to customer due diligence also requires a risk assessment to be undertaken with respect to a particular customer, based on that customer's individual circumstances. This will determine the extent of the identification and other customer due diligence information that will be sought, how it will be verified and the extent to which the resulting relationship will be monitored. The specific requirements of the Code concerning the obtaining of identification information and the verification of identity are covered later in Part 2 of the Code.

(xii) It is important to appreciate that identifying a customer as carrying a higher risk of involvement in money laundering or terrorist financing does not necessarily mean that the customer is a money launderer or financing terrorism. Similarly, identifying a customer as carrying a lower risk of involvement in money laundering or terrorist financing does not necessarily mean that the customer is not a money launderer or is not financing terrorism.

(xiii) As already indicated, the broad objective of a risk-sensitive approach is to enable a service provider to know who its customers

are, what they do, and whether or not they are likely to be engaged in money laundering, terrorist financing or other criminal activity. This is achieved by preparing a risk profile for each customer on the basis of the customer risk assessment undertaken in accordance with regulation 13(2)(b) of the Regulations.

Relationship Information

(xiv) Customer due diligence information comprises both information on the identity of the customer [identification information] and information on the business relationship [relationship information]. Identification information is covered in the following paragraphs of the Code. The Guidance Notes that follows relates to relationship information.

(xv) Relationship information (ie information on the business relationship, or proposed business relationship), is the information necessary to enable a service provider to fully understand the nature of the customer's business, or proposed business and the rationale for the business relationship. This will include information on the source of the customer's funds and, in higher risk relationships, the source of the customer's wealth.

(xvi) The nature and extent of the relationship information obtained with respect to a customer will depend on a number of factors, such as the countries with which he is connected, the product or service to be supplied how the product or service will be delivered and factors specific to the customer. The principle objective is to obtain sufficient information to identify a pattern of expected activity and to identify unusual, complex or higher risk activity and transactions that may indicate money laundering or terrorist financing. However, paragraph 5(2) of the Code sets out relationship information that must always be obtained by a service provider, in relation to a trust or legal person.

Source of funds and wealth

(xvii) The "source of funds" is the business, transaction or other activity that generates the funds for a customer, which may include the customer's occupation.

A person's "source of wealth" means the business, transactions or other activities that have generated the total net worth of a person.

(xviii) Paragraph 5(1)(c) of the Code provides that information should always be obtained with respect to the source of funds and that information with respect to the source of wealth should be obtained where the customer, business relationship or occasional transaction presents a high risk.

Information on the source of funds and source of wealth and any transaction that exceeds the value of $10,000.00 shall be documented in a form referred to as the 'Declaration of Source of Funds/Wealth' form.

(xix) When sufficient customer due diligence information has been obtained, the service provider should carry out a customer risk assessment, as required by the Regulations. Regulation 13(3) of the Regulations provides that, in preparing a customer risk assessment, a service provider must consider the following four risk elements: customer risk, product risk, delivery risk and country risk. An assessment of each of these risks is combined to produce a risk profile for the customer. These risk elements are considered below.

Customer risk

(xx) Customer risk is the identification of the risk posed by the type of customer. In assessing customer risk, a service provider will need to consider a number of factors, including the following:

(a) Type of customer: For example a politically exposed person presents a higher level of risk.

(b) Type and complexity of the relationship: Complex business structures, for example structures involving a mixture of companies and trusts or simply a number of different companies, can make it easier to conceal underlying beneficiaries. Relationships involving these structures present a higher risk unless there is a clear and legitimate commercial rationale for the structure. The use of bearer shares will also present a higher risk, particularly where the country in which the company is incorporated or registered does not require bearer shares to be immobilised.

(c) The value and nature of the funds or assets: Customers engaged in a business that generates significant amounts of cash, or wishing to undertake a large number of cash transactions, or with a high value of funds, especially where not fully explained, present a higher level of risk. The geographic source of the funds is also relevant to risk.

(d) Commercial rationale: Is there a clear commercial rationale for the customer purchasing the product or service? If there is no clear rationale, the relationship should be regarded as presenting a higher level of risk.

(e) Secrecy: Requests to associate undue levels of secrecy with a transaction or relationship or, in the case of a legal entity, reluctance to provide information as to beneficial owners or controllers present a higher level of risk.

(f) Source of funds and wealth not easily verified: Situations where the source of funds and/or the origin of wealth cannot be easily verified, or where the audit trail has been deliberately broken and/or unnecessarily layered present a higher level of risk.

(g) Delegation of authority: Delegation of authority by the customer, for example, through a power of attorney presents a higher level of risk.

(xxi) Other factors may suggest a lower level of risk, for example, where the customer:

(a) has a strong reputation;

(b) is subject to public disclosure rules, for example publicly listed companies;

(c) is subject to regulation by a statutory regulator (not just a financial services regulator).

(xxii) Regard should always be had to external data sources that may indicate whether a person is high risk. These will include directives to apply United Nations sanctions, guidance issued by the Committee and may include information published by governments and law enforcement authorities on terrorists [e.g. United States government agencies such as the Federal Bureau of Investigation and OFAC], electronic subscription databases, the internet and other media.

Product risk

(xxiii)Product risk (or service risk) is the risk posed by the product proposition itself. The following indicate higher risk products:

(a) ability to make payments to third parties;

(b) ability to pay in or withdraw cash;

(c) ability to migrate from one product to another;

(d) ability to hold boxes, parcels or sealed envelopes in safe custody;

(e) ability to use numbered accounts or accounts that offer a layer of opacity;

(f) ability to pool underlying customers.

(xxiv)The use of correspondent banking relationships is common and commercially convenient. However, this presents an increased risk as other customers of the bank may be using it to launder funds. Additional due diligence and/or controls are therefore required. Correspondent banking relationships are covered in Part 8 of the Code.

Delivery risk

(xxv)Delivery risk is the risk posed by the mechanism through which the business relationship is commenced and transacted.

The following indicate higher risk delivery mechanisms:

(a) where the relationship with the customer is indirect, for example through the use of intermediaries; and

(b) non face to face relationships, for example where products are delivered exclusively by post or telephone or over the Internet.

Country risk

(xxvi)Country risk is the risk posed by the geographic provenance of the economic activity of the business relationship. It should be noted that this is wider than the residence of the customer, third party or beneficial owner and will include, for example, the place where the business is being carried on.

(xxvii)Countries falling into one or more of the following categories should be considered as higher risk countries:

(a) countries that have inadequate safeguards in place against money laundering or terrorist financing;

(b) countries that have high levels of organised crime;

(c) countries that have strong links with terrorist activities;

(d) countries that are vulnerable to corruption;

(e) countries that are the subject of United Nations or European Union sanctions.

(xxviii) In assessing which countries may present a higher risk, regard should be had to objective data published, for example, by the IMF, FATF, US Department of State (International Narcotics Control Strategy Report), Office of Foreign Assets Control ("OFAC"), and Transparency International (Corruption Perception Index).

Customer Risk Assessment

(xxix)In preparing a customer risk assessment, a service provider should take into account:

(a) the customer due diligence information obtained and the evaluation of that information; and

(b) inconsistencies between the customer due diligence information obtained.

(xxx)The sophistication of the risk assessment process may be determined according to factors established by the business risk assessment. Where it is appropriate to do so, risk may be assessed generically for applicants and customers falling into similar categories. The business of some service providers, their products, and customer base, can be relatively simple, involving few products, with most applicants or customers falling into similar risk categories. In such circumstances, a simple approach, building on the risk that the business' products are assessed to present, may be appropriate for most customers, with the focus being on those customers who fall outside the norm.

Others may have a greater level of business, but large numbers of their customers may be predominantly retail, served through delivery channels that offer the possibility of adopting a standardised approach to many procedures. Again, the approach for most customers may be relatively straight forward, building on product risk.

A more complex system may be appropriate for diverse customer bases or service providers with broad ranges of products or services.

Updating customer due diligence

(xxxi) Regulation 11(1)(b) of the Regulations requires a service provider to apply customer due diligence measures subsequent to the establishment of a business relationship (ie to update the customer due diligence) where the service provider:

(a) suspects money laundering or terrorist financing;

(b) doubts the veracity or adequacy of documents, data or information previously obtained under its customer due diligence measures or when conducting ongoing monitoring;

(c) at other appropriate times to existing customers as determined on a risk-sensitive basis.

(xxxii) In order to demonstrate compliance with paragraph (xxxi)(c), the Committee would usually expect a service provider to:

(a) review and update its customer due diligence information on at least an annual basis where it has assessed a customer relationship as presenting a higher risk; and

(b) review and update its customer due diligence information on a risk-sensitive basis, but not less than once in every 3 years, where it has assessed a customer relationship as presenting a normal or low risk.

Events such as the opening of a new account, the purchase of a further product, or meeting with a customer may present a convenient opportunity to update customer due diligence information.

Foreign politically exposed persons

6. (1) A service provider shall establish, maintain and implement appropriate risk management systems to determine whether a customer, third party or beneficial owner is a foreign politically exposed person and those risk management systems shall take into account that a person may become a foreign politically exposed person after the establishment of a business relationship.

(2) A service provider shall ensure that no business relationship is established with a foreign politically exposed person, or where the third party or beneficial owner is a foreign politically exposed person, unless the prior approval of the board or senior management has been obtained.

(3) Where a service provider has established a business relationship with a customer and the customer, a third party or beneficial owner is subsequently identified as a foreign politically exposed person, the business relationship shall not be continued unless the approval of the board or senior management has been obtained.

(4) Subparagraph (3) applies whether the customer, third party or beneficial owner:

(a) was not a foreign politically exposed person at the time that the business relationship was established, but the person was subsequently identified as a foreign politically exposed person; or

(b) becomes a foreign politically exposed after the establishment of the business relationship.

(5) A service provider shall take reasonable measures to establish the source of wealth and the source of funds of customers, third parties and beneficial owners identified as foreign politically exposed persons.

(6) Subparagraphs (1) to (5) apply in relation to a person who is a family member or close associate of a foreign politically exposed person, as if the person was a foreign politically exposed person.

Other politically exposed persons, family members and close associates

7. (1) A service provider shall take reasonable measures to determine whether a customer, third party or beneficial owner is:

(a) a domestic politically exposed person;

(b) a person who is, or has been, entrusted with a prominent function by an international organisation; or

(c) a family member or close associate of a person referred to in sub-subparagraph (a) or (b).

(2) Where a service provider is required to apply enhanced due diligence measures or undertake enhanced ongoing monitoring in relation to a person specified in subparagraph (1)(a), (b) or (c), paragraph 6 applies as if the person was a foreign politically exposed person.

GUIDANCE NOTES

Enhanced customer due diligence - introduction

(i) Regulation 14(2) of the Regulations requires a service provider, on a risk-sensitive basis to apply enhanced customer due diligence measures (and undertake enhanced ongoing monitoring) in the following specified circumstances:

(a) where the customer has not been physically present for identification purposes;

(b) where the service provider has, or proposes to have, a business relationship with, or proposes to carry out an occasional transaction with, a person connected with a country or territory that does not apply, or insufficiently applies, the FATF Recommendations;

(c) where the service provider is a SVG bank that has or proposes to have a banking or similar relationship with an institution whose address for that purpose is outside St Vincent and the Grenadines;

(d) where the service provider has or proposes to have a business relationship with, or to carry out an occasional transaction with, a politically exposed person;

(e) where any of the following is a politically exposed person or a family member or close associate of a politically exposed person:

(I) a beneficial owner of the customer or a third party;

(II) a third party;

(III) a person acting, or purporting to act, on behalf of the customer;

(IV) where a customer, transaction or business relationship involves (i) private banking, legal persons or arrangements, including trusts, that are personal asset holding vehicles; or (ii) companies that have nominee shareholders or shares in bearer form; and

(V) in any other situation which by its nature can present a higher risk of money laundering or terrorist financing.

(ii) Enhanced ongoing monitoring is also required in any other situation which, by its nature can present a higher risk of money laundering or terrorist financing. A service provider must decide whether a particular situation can present a higher risk of money laundering using the customer risk assessment that it is required to carry out. However, certain factors should always be considered to indicate higher level of risk, such as:

(a) customers who are connected with business sectors that are vulnerable to corruption, for example arms or oil sales; and

(b) customers who are connected to countries that are perceived to have a higher level of corruption (see the further the Guidance notes below with respect to politically exposed persons).

Enhanced customer due diligence measures and ongoing monitoring

(iii) Regulation 14(1) of the Regulations provides that:

"'"enhanced customer due diligence measures" and "enhanced ongoing monitoring" mean customer due diligence measures, or ongoing monitoring, that involve specific and adequate measures to compensate for the higher risk of money laundering or terrorist financing.".

(iv) Where a service provider is required by the Regulations to apply enhanced due diligence measures and undertake enhanced ongoing monitoring, the service provider must determine, on the basis of the particular circumstances, what "specific and adequate measures" will be required to compensate for the higher money laundering and terrorist financing risks. These measures are almost certain to include obtaining further identification information

and relationship information, including further information on the source of funds and the source of wealth. These should be obtained from appropriate sources, which may be the customer or an independent source.

(v) Other enhanced due diligence measures that should be considered include:

(a) taking additional steps to verify the customer due diligence information obtained;

(b) obtaining due diligence reports from independent experts to confirm the veracity of customer due diligence information held;

(c) requiring board or senior management approval for higher risk customers;

(d) requiring more frequent reviews of high risk business relationships; and

(e) setting lower monitoring thresholds for transactions connected with the business relationship.

Politically exposed persons

(vi) Politically exposed persons [or "PEPs"] are individuals who are, or have been, entrusted with prominent public functions whether in St Vincent and the Grenadines or in a foreign country, and who are, or have been, entrusted with a prominent function by an international organisation, together with their immediate family members and their close associates.

(vii) PEPs present a high risk to service providers because their position makes them vulnerable to corruption and corruption is invariably associated with money laundering. The risk to a service provider is even higher where the PEP has connections with countries, or types of business, where corruption is prevalent. The FATF Recommendations therefore require all PEPs to be regarded as high risk customers. Although PEP status places a customer into a higher risk category, it does not, of itself, incriminate the person concerned.

(viii) The Regulations provide a comprehensive definition of a PEP [regulation 8]. It should be noted that the definition includes, not

just the individual who has a prominent function in government, but also one who has a prominent function in an international organisation and those people's immediate family members and close associates. Regulation 8(4) provides a definition of "international organisation". Examples of international organisations include the United Nations and affiliated international organisations; regional international organisations such as the Organisation of Eastern Caribbean States, the Council of Europe, institutions of the European Union and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization, and economic organisations such as the World Trade Organisation, the Caribbean Community (CARICOM), etc.

(ix) Regulation 14(2) of the Regulations requires a service provider, on a risk-sensitive basis, to apply enhanced due diligence measures and undertake enhanced ongoing monitoring where a customer, third party or beneficial owner is a PEP and paragraphs 6 and 7 of the Code supplement these provisions by setting out a number of detailed additional requirements with respect to PEPs.

(x) Establishing whether a person is a PEP is not always straightforward and can present difficulties. The risk assessment carried out in compliance with paragraph 2 of the Code will assist a service provider to determine the extent to which PEPS are a significant risk to it. PEPs will present a greater risk to some service providers than to others, depending in part on their business and delivery channels. Whilst the requirements of the Regulations and the Code apply to all service providers, where the business assessment indicates that a service provider faces a more significant risk, it will need to take that into account in designing its systems and controls with respect to PEPs.

(xi) The following checks may assist a service provider to determine whether a person is a PEP:

(a) Assess the corruption risks posed by any countries with which the person has a connection. There are a number of specialist reports and databases published by specialised national, international, non-governmental and commercial organisations that may be used for this purpose. One potential reference resource is the Transparency

International Corruption Perception Index, which ranks approximately 150 countries according to their perceived level of corruption.

(b) If, on a risk-sensitive basis, the service provider needs to conduct more thorough checks, or if there is a high likelihood of a service provider having PEPs as customers, subscription to a specialist PEP database may be the only adequate risk mitigation tool.

(c) Ascertain the identity of individuals who hold, or formerly held, prominent public functions in any country with which the person concerned is connected and, as far as reasonably practicable, determine whether the person concerned has any associations with those individuals. The Websites of international organizations, such as the UN, may assist in determining the identity of such individuals.

(xii) The above checks do not represent a comprehensive list and the Committee would expect them to be used on a risk-sensitive basis. The extent to which a service provider needs to utilize the checks, if at all, will depend upon its business risk assessment and its customer risk assessment.

(xiii) Although new and existing customers may not initially meet the definition of a PEP, service providers should, as far as practicable, be alert to public information relating to possible changes in the status of its customers with regard to political exposure.

Identification information, individuals

8. (1) A service provider shall obtain the following identification information with respect to an individual who it is required by the Regulations or this Code to identify:

(a) the full legal name of, any former names of and any other names used by the individual;

(b) the gender of the individual;

(c) the principal residential address of the individual; and

(d) the date of birth of the individual.

(2) Where a service provider determines that an individual who it is required to identify presents a higher level of risk, the service provider shall obtain additional identification information with respect to the individual.

(3) The additional identification information to be obtained with respect to a higher risk individual shall include at least two of the following:

(a) the individual's place of birth;

(b) the individual's nationality;

(c) an official government issued identity number or other government identifier.

Verification of identity, individuals

9. (1) A service provider shall:

(a) verify the identity of an individual where required by the Regulations or this Code to do so; and

(b) take reasonable measures to re-verify an aspect of an individual's identity if it changes after the individual's identity has been verified.

(2) Without limiting subparagraph (1) (b), the following represent changes of an individual's identity within the meaning of that paragraph:

(a) marriage;

(b) change of nationality;

(c) change of address.

(3) Where a service provider determines that an individual whose identity it is required to verify presents a low risk, the service provider shall, using evidence from at least one independent source, verify:

(a) the individual's full legal name, any former names and any other names used by the individual; and

(b) either:

(i) the principal residential address of the individual, or

(ii) the individual's date of birth.

(4) Where a service provider determines that an individual whose identity it is required to verify presents a higher level of risk, the

service provider shall, using evidence from at least two independent sources, verify:

(a) the individual's full legal name, any former names and any other names used by the individual;

(b) the principal residential address of the individual; and

(c) the individual's:

(i) date of birth;

(ii) place of birth;

(iii) nationality; and

(iv) gender.

(5) Where a service provider determines that an individual whose identity it is required to verify presents a high level of risk, the service provider shall, using evidence from at least two independent sources of the best forms of identification, verify the individual's:

(a) nationality or address; and

(b) government issued identity number or other government identifier.

(6) A document used to identify the identity of an individual must be in a language understood by those employees of the service provider who are responsible for verifying the individual's identity.

(7) The best forms of identification for an individual are:

(a) a current passport;

(b) a current national government issued identification card; and

(c) a current driving licence;

Introduction

(i) Paragraphs 10 to 17 of the Code provide for, and the following Guidance Notes describes:

(a) the identification information that must be obtained by a service provider in applying customer due diligence measures and ongoing monitoring;

(b) the verification of the identity information; and

(c) exceptions to the requirements to obtain and verify identity information.

These Guidance Notes also covers the requirements of the Regulations concerning the obtaining and verification of identity evidence.

Requirements of the Regulations

(ii) As indicated in the Guidance Notes to previous paragraphs of the Code, the Regulations [regulation 6(1)] provide that the customer due diligence measures to be applied by a service provider include:

(a) identifying the customer, any third parties and any beneficial owners;

(b) verifying the identity of the customer and any third parties; and

(c) taking reasonable measures, on a risk-sensitive basis, to verify the identity of each beneficial owner of the customer and any third parties.

(iii) In essence, all persons who are not individuals, including companies, foundations, partnerships ***or*** *trusts and any other type of arrangement are regarded as having a beneficial owner who is an individual. The definition of "beneficial owner" is contained in regulation 4 of the Regulations which, in summary, provides that beneficial owners are:*

(a) individuals who are ultimate beneficial owners of the legal person, partnership or arrangement; and

(b) individuals who exercise ultimate control over the management of the legal person, partnership or arrangement.

(iv) It should be noted that it makes no difference whether:

(a) an individual's ultimate ownership or control of a legal person, partnership or arrangement is direct or indirect; or

(b) an individual is the sole beneficial owner or a joint beneficial owner.

(v) As indicated in the guidance notes to the paragraphs on customer due diligence above, regulation 11 of the Regulations specifies when customer due diligence measures must be applied. These circumstances are supplemented by paragraph 4 of the Code.

(vi) Although customer due diligence measures must in most cases be applied before the establishment of a business relationship or the carrying out of an occasional transaction, regulation 11(3) and (4) of the Regulations permit two exceptions. Subregulation (3) provides that a service provider may complete the verification of the identity of a customer, third party or beneficial owner after the establishment of a business relationship if:

(a) it is necessary not to interrupt the normal conduct of business;

(b) there is little risk of money laundering or terrorist financing occurring as a result; and

(c) verification of identity is completed as soon as reasonably practicable after the contact with the customer is first established.

(vii) Regulation 11(4) of the Regulations permits a bank to verify the identity of a bank account holder after the opening of the bank account provided that there are adequate safeguards in place to ensure that, before verification has been completed:

(a) the account is not closed; and

(b) transactions are not carried out by or on behalf of the account holder, including any payment from the account to the account holder.

(viii) These are the only exceptions. In all other cases, customer due diligence measures must be applied before the establishment of a business relationship or the carrying out of an occasional transaction.

Identification information

(ix) Customer identification is a two-stage process. First it is necessary to obtain identity information, that is, information concerning the

identity of the person concerned. Next, the identity information must be verified.

The objective of obtaining identity information is to establish that the named person actually exists.

The objective of the second stage is to verify from reliable, independent documentary or other acceptable evidence that the person concerned is that person.

(x) The identity of a person has a number of different aspects. In respect of an individual, identity includes the individual's full name (which may change), gender and date and place of birth. Other facts about an individual may also be relevant, including family circumstances and addresses, employment and career, contacts with Government and other authorities and with other financial institutions, in and outside St Vincent and the Grenadines, and physical appearance. In respect of a legal entity, identity is a combination of its constitution, its business and its legal and ownership structure.

Identification of an individual

(xi) A service provider is required by the Regulations to obtain identification on, and verify the identity of, any individual:

(a) who, as a customer, seeks to enter into a business relationship with the service provider or undertake an occasional transaction, whether solely or jointly;

(b) who is a third party; or

(c) who is the beneficial owner of a customer or of a third party;

(xii) Paragraph 8(1) of the Code sets out the identification that must always be obtained with respect to an individual. Paragraph 8(2) requires a service provider to obtain additional identity information where it determines that the individual presents a higher risk and paragraph 8(3) specifies additional identification information that must be obtained. Although a service provider is only required to obtain two types of additional identification information, a service provider should consider whether it should obtain all three and, where it only obtains two of the specified

types, it should consider obtaining a third (different) type of identification information.

Verification of identity of an individual

(xiii) It is an overriding requirement of both the Regulations and the Code that a service provider verifies the identity of a person using documents, data or information obtained from a reliable and independent source.

(xiv) Evidence of identity can take a number of forms. In respect of individuals, much weight is to be placed on identity documents, such as passports and government issued identification as these are often the easiest way of being reasonably satisfied as to an individual's identity. It is, however, possible to be reasonably satisfied as to a customer's identity based on other forms of evidence. However, service providers should appreciate that different sources of identification evidence vary in their integrity and independence. For example, some documents are issued after a due diligence check, for example passports, whilst others are not. Also, some documents are more easily forged. Therefore, a service provider should not engage in the practice of accepting forms of identity evidence that are not subject to rigorous due diligence checks. Service providers should apply the provisions of the code in light of the best practice stipulated by the FATF Recommendations and issued by the Committee.

(xv) Given the range of sources available to a service provider, and the risk profiles of different customers, the Code is not prescriptive as to how the identity of any person should be verified. However a service provider should be able to demonstrate that it has complied with its obligations to verify the identity of an individual if it follows the Guidance Notes set out in the following paragraphs. Service providers are reminded that section 168(4) of the Act provides that, in deciding whether a person has committed an offence under the Regulations, the Court shall consider whether the person has followed any guidance issued by the Committee.

(xvi) The Committee regards the following general methods of verifying the identity of an individual to be acceptable and as the best forms of indentification:

(a) a current passport, which provides photographic evidence of identity;

(b) a current national identity card or document, but only if it provides photographic evidence of identity;

(c) a current driving licence, but only if the licensing authority carries out an identity check before issuing the licence and the licence provides photographic evidence of identity;

(d) an independent data source (including an electronic source), subject to the Guidance Notes on independent data sources that follows.

(xvii) The Committee considers the following methods of verifying an individual's residential address to be acceptable:

(a) a recent bank statement or utility bill;

(b) correspondence from a central or local government department or agency;

(c) a letter of introduction confirming residential address from a regulated person or a foreign regulated person; or

(d) a personal visit to the individual's residential address.

(xvii) Where the general methods of identifying the identity of an individual are not practical and the individual concerned presents a low risk, the individual's identity shall first be verified using:

(a) a current national identity card or document, but only if it provides photographic evidence of identity or a full (ie not a temporary) driver's licence issued in St Vincent and the Grenadines; or

(b) a birth certificate, in conjunction with:

(I) a recent bank statement or utility bill;

(II) documentation issued by a government source; or

(III) a letter of introduction from a regulated person.

The use of independent data sources

(xix) A service provider may be able to rely on an independent data source to provide satisfactory evidence of identity, or an aspect of it. Data sources include both sources of reliable independent

public information, such as a register of electors or a telephone directory, commercially available databases maintained by, for example, credit reference agencies, business information services and commercial agencies that provide electronic identity checks.

(xx) In principle, the Committee regards such independent data sources as acceptable for the verification of the identity. However, where a service provider uses an independent data source or sources, the Committee would expect the service provider to ensure that:

(a) the source, scope and quality of the data are satisfactory;

(b) to obtain at least two matches of each component of an individual's identity being verified; and

(c) it is able to capture and record the information used to verify identity.

(xxi) In considering whether an independent third party data source is satisfactory, a service provider should consider the following:

(a) whether the third party is registered with a data protection agency;

(b) the range of positive information sources that the third party can call upon to link an applicant to both current and historical data;

(c) whether the third party accesses negative information sources such as databases relating to fraud and deceased persons;

(d) whether the third party accesses a wide range of alert data sources; and

(e) whether the third party has transparent processes that enable a service provider to know what checks have been carried out, what the results of these checks were and to be able to determine the level of satisfaction provided by those checks.

Identification information, legal persons (other than foundations)

10. (1) This paragraph and paragraphs 11 and 12 apply to a legal person other than a foundation.

(2) A service provider shall obtain the following identification information with respect to a legal person that it is required by the Regulations or this Code to identify:

(a) the full name of the legal person and any trading names that it uses;

(b) the date of the incorporation, registration or formation of the legal person;

(c) any official identifying number;

(c) the registered office or, if it does not have a registered office, the address of the head office of the legal person;

(d) the name and address of the registered agent of the legal person (or equivalent), if any;

(e) the mailing address of the legal person;

(f) the principal place of business of the legal person;

(g) the names of the directors of the legal person;

(h) identification information on those directors who have authority to give instructions to the service provider concerning the business relationship or occasional transaction; and

(i) identification information on individuals who are the ultimate holders of 15% or more of the legal person.

(3) Where a service provider determines that a legal person that it is required to identify presents a higher level of risk, the service provider shall obtain such additional identification information with respect to the legal person as it consider appropriate.

(4) Where subparagraph (3) applies, but without limiting it, a service provider shall obtain identification information on every director of the legal person.

(5) Where identification information on an individual, as a director or beneficial owner, is required to be obtained, paragraph 8 applies.

Verification of identity, legal persons (other than foundations)

11. (1) A service provider shall:

(a) verify the identity of a legal person where required by the Regulations to do so; and

(b) take reasonable measures to verify the identity of the beneficial owners of the legal person.

(2) Where a service provider determines that a legal person, the identity of which it is required to verify, presents a low risk, the service provider shall, using evidence from at least one independent source verify:

(a) the name of the legal person;

(b) the official identifying number; and

(c) the date and country of its incorporation, registration or formation.

(3) Where a service provider determines that a legal person, the identity of which it is required to verify, presents a higher level of risk, the service provider shall verify:

(a) the address of the registered office, or head office, of the legal person, as applicable; and

(b) the address of the principal place of business of the legal person, if different from its registered office or head office.

(4) Where a service provider determines that a legal person, the identity of which it is required to verify, presents a high level of risk, the service provider shall verify such other components of the legal person's identification as it considers appropriate.

(5) A document used to identify the identity of a legal person or its beneficial owners must be in a language understood by those employees of the service provider who are responsible for verifying their identity.

Verification of directors and beneficial owners

12. (1) A service provider shall in all cases verify the identity of any director of the legal person specified in paragraph 10(2) (h).

(2) Where the service provider determines that the legal person presents more than a low level of risk, it shall verify such additional components of the identity of the legal person as it considers appropriate.

(3) Where subparagraph (2) applies, but without limiting it, a service provider shall verify the identity of each director and each beneficial owner of the legal person.

(4) Where the identity of an individual, as director or beneficial owner, is required to be verified, paragraph 8 applies.

GUIDANCE NOTES

Introduction

(i) Paragraphs 10 to 12 of the Code specify requirements concerning the identification of, and the verification of the identity of, legal persons, other than foundations. Foundations are covered in paragraphs 15 to 17 of the Code. A legal person is defined in the Regulations to include a company, a partnership, whether limited or general, an association or any unincorporated body of persons, but it does not include a trust. The definition therefore extends beyond its natural meaning and includes clubs, societies, charities, church bodies and institutes, amongst others.

Identification of a legal person

(ii) There is a wide range of potential customers that are not individuals. These include legal persons (such as companies) and trusts (which are not entities and are covered separately in paragraphs 13 and 14 of the Code). The legal owners of a legal person may be specific individuals or other legal persons. However, the beneficial ownership may rest with others, either because the legal owner is acting for the beneficial owner, or because there is a legal obligation for the ownership to be registered in a particular way.

(iii) In deciding who the customer is when it is not an individual, the objective of a service provider must be to know who has control over the funds, which form or otherwise relate to the relationship, and/or form the controlling mind and/or management of any legal person involved in the funds. The subsequent judgment as to whose identity to verify will be made following a risk-based approach and will take account of the number of individuals, the nature and distribution of their interests in the entity and the nature and extent of any business, contractual or family relationship between them.

(iv) Certain information about the legal person comprising the non-individual customer should be obtained as a standard

requirement. Thereafter, on the basis of the money laundering/ terrorist financing risk assessed through the customer risk assessment, a service provider should decide the extent to which the identity of the person and of specific individuals should be verified, using reliable, independent source documents, data or information. The service provider should also decide what additional information in respect of the legal person and, potentially, some of the individuals behind it should be obtained.

(v) Whilst information on a legal person's website may be useful, service providers will understand that that this information should be treated with caution as it has not been independently verified before being made publicly available on the Internet.

(vi) Where the person seeking to establish a business relationship or carry out an occasional transaction is a legal person, a service provider should ensure that it fully understands the legal form, structure and ownership of the legal person and should obtain sufficient additional information on the nature of the person's business, and the reasons for seeking the product or service.

(vii) A service provider is required by the Regulations to obtain identification information on, and verify the identity of, any legal person:

(a) that, as a customer, seeks to enter into a business relationship with the service provider or undertake an occasional transaction, whether solely or jointly; or

(b) that is a third party;

(viii) Paragraph 10(2) of the Code sets out the identification that must always be obtained with respect to a legal person. Paragraph 10(3) requires a service provider to obtain additional identity information where it determines that the legal person presents a higher risk.

Verification of identity of a legal person

(ix) The Committee regards the following general methods of verifying the identity of a legal person and the powers that regulate or bind the legal person to be acceptable:

certificate of incorporation, registration or equivalent;

a certificate of good standing from the Regulator of the legal person;

A partnership agreement;

memorandum and articles of association or equivalent constituting documents;

a company registry search, including confirmation that the legal person is not in the process of being dissolved, struck off, wound up or terminated;

the latest audited financial statements of the legal person;

independent data sources, including electronic sources, e.g. business information services; and

where the service provider determines that the legal person does not present a low risk, a personal visit to the legal person's principal place of business.

(x) Where the service provider determines that the legal person presents a low level of risk, at least one of the methods specified above should be used. Where it determines that the legal person presents a higher level of risk, at least two of the methods specified above should be used.

(xi) In the case of unincorporated bodies of persons, such as clubs, a service provider will need to identify the persons who fulfil equivalent functions to the directors of a company, such as the members of the board or governing council.

(xii) Where a service provider verifies the identity of a director, or equivalent, on a remote basis, paragraph 18 of the Code applies.

(xiii) In the case of a legal person that is a regulated person, the identity of a director may be verified if the full name of the director is obtained together with written confirmation from the regulated person that the person concerned is a director.

Identification information, trusts and trustees

13. (1) [Subject to subsection (2)], where a service provider is required by the Regulations or this Code to identify a trust, it shall:

(a) obtain the following identification information:

(i) the name of the trust,

(ii) the date of the establishment of the trust,

(iii) any official identifying number,

(iv) identification information on each trustee of the trust,

(v) the mailing address of the trustees,

(vi) identification information on each settlor of the trust,

(vii) identification information on each beneficiary or class of beneficiaries of the trust, except a trust to which subparagraph (2) or (3) applies.

(viii) identification information on each protector or enforcer of the trust;

(ix) Identification of any other natural person(s) exercising ultimate effective control over the trust; and

(b) obtain confirmation from the trustees that they have provided all the information requested and that they will update the information in the event that it changes.

(2) In the case of a discretionary trust or a trust with one or more types or classes of beneficiaries, the service provider shall obtain information concerning the type or class of beneficiary that is sufficient to enable the identity of a beneficiary to be established at the time the beneficiary receives any property or benefit from the trust or exercises a vested right.

(3) In the case of a charitable trust or purpose trust, the service provider must obtain information on the objects of the trust.

(4) For the purpose of this Code, "settlor" includes a person who, as settlor, established the trust and any person who has, at any time, subsequently settled assets into the trust.

(5) Identification information required to be obtained on any person under this paragraph shall be obtained in accordance with paragraph 8 if the person is an individual, paragraph 10 if the person is a

legal person, other than a foundation, or paragraph 15 if the person is a foundation.

Verification of identity, trusts and trustees

14. (1) Where a service provider is required by the Regulations or this Code to verify the identity of a trust, it shall verify:

(a) the name and date of establishment of the trust;

(b) the identity of each trustee, settlor and protector or enforcer of the trust; and

(c) the appointment of the trustee and the nature of his duties.

(2) Where a service provider determines that a trust, the identity of which it is required to verify, presents a higher level of risk, the service provider shall:

(a) take reasonable measures to verify the identity of each person specified in paragraph 13(5) and

(b) verify such other components of the legal person's identification as it considers appropriate.

(3) A document used to verify the identity of a trust or a person specified in this paragraph must be in a language understood by those employees of the service provider who are responsible for verifying the identity of the trust or person concerned.

(4) A person whose identity is required by this paragraph to be verified shall:

(a) if the person is an individual, be verified in accordance with paragraph 9;

(b) if the person is a legal person, be verified in accordance with paragraph 11; or

(c) if the person is a foundation, be verified in accordance with paragraph 16.

Introduction

(i) There are a wide variety of trusts, ranging from large, nationally and internationally active organisations subject to a high degree of public interest and quasi-accountability, through to trusts set up under testamentary arrangements, and trusts established for wealth management purposes. It is important, in putting proportionate anti-money laundering or prevention of terrorism financing policies, procedures, systems and controls in place, and in carrying out risk assessments, that service providers take account of the different money laundering or terrorist financing risks that trusts of different sizes and areas of activity present.

(ii) Trusts are not separate legal entities – it is the trustees collectively who are the customer. In these cases, the obligation to identify the customer attaches to the trustees, rather than to the trust itself, although certain identification information concerning the trust is also required to be obtained. The purpose and objects of most trusts are set out in a trust deed.

(iii) A trustee will also have to be identified and verified where a trustee is the beneficial owner or the controller of an applicant for business or is a third party on whose behalf an applicant for business is acting.

(iv) A service provider is not required to establish the detailed terms of the trust, nor the rights of the beneficiaries.

(v) The Regulations require a service provider to obtain identification information concerning a trust when the trustee of a trust (in that capacity) is:

(a) a customer;

(b) a third party; or

(c) a beneficial owner.

(vi) As provided by the Code, the relevant paragraphs of the Code relating to individuals, legal persons or foundations apply depending upon whether the trustee whose identity information

is required to be obtained, or whose identity is required to be verified, is an individual, a legal person or a foundation.

Identification information, foundations

15. (1) A service provider shall obtain the following identification information with respect to a foundation that it is required by the Regulations or this Code to identify:

(a) the full name of the foundation;

(b) the date and country of the establishment, registration, formation or incorporation of the foundation;

(c) any official identifying number;

(d) the registered address, or equivalent, of a foundation or, if a foundation does not have a registered address (or equivalent), the address of the head office of the foundation;

(e) the mailing address of the foundation, if different from its registered address or equivalent;

(f) the principal place of business of the foundation, if different from its registered address or equivalent;

(g) the name and address of the registered agent (or equivalent) of a foundation, if any;

(h) the name and address of the Secretary, or equivalent, of a foundation, if any;

(i) the names of the Foundation Council members (or equivalent) and, if any decision requires the approval of any other persons, the names of those persons;

(j) identification information on those Foundation Council members (or equivalent) who have authority to give instructions to the service provider concerning the business relationship or occasional transaction;

(k) identification information on the guardian of the foundation (or equivalent), if any;

(l) identification information on the founder or founders, on any other person who has contributed to the assets

of the foundation and on any person to whom the rights of the founder or founders have been assigned.

(2) Where a service provider determines that a foundation that it is required to identify presents a higher level of risk, the service provider shall obtain such additional identification information with respect to the foundation as it consider appropriate.

(3) Where subparagraph (2) applies, but without limiting it, a service provider shall obtain identification information on:

(a) every Foundation Council member of the foundation, or equivalent;

(b) any other persons whose approval is required for any decision; and

(c) any beneficiaries of the foundation.

(4) Identification information required to be obtained on any person under this paragraph shall be obtained in accordance with paragraph 8 if the person is an individual or paragraph 10 if the person is a legal person.

Verification of identity, foundations

16. (1) Where a service provider is required by the Regulations or this Code to verify the identity of a foundation, it shall:

(a) verify the identity of the foundation; and

(b) take reasonable measures to verify the identity of persons concerned with the operation of the foundation.

(2) Where a service provider determines that a foundation the identity of which it is required to verify presents a low risk, the service provider shall, using evidence from at least one independent source, verify:

(a) the name of the foundation and any official identifying number; and

(b) the date and country of the foundation's establishment, registration, formation or incorporation.

(3) Where a service provider determines that a foundation, the identity of which it is required to verify, presents a higher level of risk, the service provider shall verify:

(a) the registered address or head office of the foundation, or the equivalent, of in the case of an overseas foundation that does not have a registered address (or equivalent), the address of the head office of the foundation; and

(b) the address of the principal place of business of the foundation, if different from its registered office or head office.

(4) Where a service provider determines that a foundation, the identity of which it is required to verify, presents a high level of risk, the service provider shall verify such other components of the foundation's identification as it considers appropriate.

(5) A document used to identify the identity of a foundation or persons concerned with the foundation must be in a language understood by those employees of the service provider who are responsible for verifying their identity.

(6) A person whose identity is required by this paragraph or paragraph 17 to be verified shall:

(a) if the person is an individual, be verified in accordance with paragraph 9; or

(b) if the person is a legal person, be verified in accordance with paragraph 11.

Verification of persons concerned with a foundation

17. (1) A service provider shall in all cases verify the identity of:

(a) any Foundation Council member (or equivalent) specified in paragraph 15(1)(j);

(b) the founder or founders, or any other person who has contributed to the assets of the foundation and on any person to whom the rights of the founder or founders have been assigned; and

(c) the guardian of the foundation (or equivalent).

(iv) A service provider is required by the Regulations to obtain identification information on, and verify the identity of, any foundation:

(a) that, as a customer, seeks to enter into a business relationship with the service provider or undertake an occasional transaction, whether solely or jointly; or

(b) that is a third party.

(v) Paragraph 15(1) of the Code sets out the identification that must always be obtained with respect to a foundation. Paragraph 15(2) requires a service provider to obtain additional identity information where it determines that the foundation presents a higher risk.

(vi) The Committee regards the following general methods of verifying the identity of a foundation to be acceptable:

(a) the declaration of establishment (or equivalent);

(b) a search of the Registry of Foundations in the country in which it is established, formed, registered or incorporated, including confirmation that the foundation is not in the process of being dissolved or struck off (or the equivalent);

(c) the latest audited financial statements of the foundation;

(d) independent data sources, including electronic sources, e.g. business information services; and

(e) where the service provider determines that the foundation does not present a low risk, a personal visit to the foundation's principal place of business.

(vii) Where the service provider determines that the foundation presents a low level of risk, at least one of the methods specified above should be used. Where it determines that the foundation presents a higher level of risk, at least two of the methods specified above should be used.

(viii) Where a service provider verifies the identity of a person concerned with the foundation on a remote basis, paragraph 18 of the Code applies.

Non face-to-face business

18. Where a service provider applies customer due diligence measures to, or carries out ongoing monitoring with respect to, an individual who is not physically present, the service provider, in addition to complying with the Regulations and this Code with respect to customer due diligence measures, shall:

(a) perform at least one additional check designed to mitigate the risk of identity fraud; and

(b) apply such additional enhanced customer due diligence measures or undertake enhanced ongoing monitoring, as the service provider considers appropriate (if any).

Certification of documents

19. (1) A service provider shall not rely on a document as a certified document unless:

(a) the document is certified by an individual who is subject to professional rules of conduct which provide the service provider with a reasonable level of comfort as to the integrity of the certifier;

(b) the individual certifying the document certifies that:

(i) he or she has seen original documentation verifying the person's identity or residential address,

(ii) the copy of the document (which he certifies) is a complete and accurate copy of that original, and

(iii) where the documentation is to be used to verify identity of an individual and contains a photograph, the photograph contained in the document certified bears a true likeness to the individual requesting certification;

(c) the certifier has signed and dated the copy document, and provided adequate information so that he may be contacted in the event of a query; and

(d) in circumstances where the certifier is located in a higher risk jurisdiction, or where the service provider has some doubts as to the veracity of the information or documentation provided by the applicant, the service provider has taken steps to check that the certifier is real.

Non-Face to Face Identification and Verification Procedures

(i) Face to face to contact with an applicant presents the lowest risk to a service provider. This is because face to face contact enables the staff of the service provider to verify the likeness of the applicant to the photograph on the documentary evidence and to identify any inconsistencies.

(ii) It follows that any mechanism that enables an applicant to apply for a product without face to face contact increases the risk to the service provider. Indeed, many service providers only accept applications remotely and do not offer them the opportunity of attending the service provider's premises. Non-face to face applications are now increasingly common as applications are made and accepted by post, telephone or via the Internet.

(iii) Although applications and transactions undertaken across the internet may, in themselves, not pose any greater risk than other non face-to-face business, such as applications submitted by post, there are other factors that may, taken together, aggravate the typical risks, for example:

(a) the ease of access to the facility, regardless of time and location;

(b) the ease of making multiple fictitious applications without incurring extra cost or the risk of detection;

(c) the absence of physical documents; and

(d) the speed of electronic transactions.

(iv) The extent of verification in respect of non face-to-face customers will depend on the nature and characteristics of the product or service requested and the assessed money laundering and terrorist financing risk presented by the customer. There are some circumstances where the applicant is typically not physically present, such as when purchasing some types of collective investments, which would not in themselves increase the risk attaching to the transaction or activity. A service provider should take account of such cases in developing their systems and procedures.

(v) Where a prospective customer approaches a service provider remotely (by post, telephone or over the internet), the service provider should carry out non face-to-face verification, either electronically or by reference to documents.

(vi) Non face-to-face identification and verification carries an inherent risk of identity fraud. Therefore, the Code requires a service provider to perform at least one additional check which is designed to mitigate the risk of identity fraud. The Code is not prescriptive as to the additional checks or checks that should be carried out as this is for the service provider to determine, depending upon the circumstances and its customer risk assessment. However, the additional checks that can be taken include:

(a) verification of identity using a further method of verification;

(b) obtaining copies of identification documents certified by a suitable certifier;

(c) requiring the first payment for the financial services product or service to be drawn on an account in the customer's name at a bank that is a regulated person or a foreign regulated person;

(d) verifying additional aspects of identity or other customer due diligence information from independent sources;

(e) telephone contact with the customer on a home or business number which has been verified prior to establishing a relationship, or telephone contact before transactions are permitted, using the call to verify additional aspects of identification information that have previously been provided;

(f) internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address; and

(g) specific card or account activation procedures.

Certification of documents

(vii) The use of a certifier guards against the risk that copy documentation provided is not a true copy of the original document and that the documentation does not correspond to the customer whose identity is to be verified. For certification to be effective, the certifier will need to have seen the original documentation and, where documentation is to be used to provide satisfactory evidence of identity for an individual, have met the individual (where certifying evidence of identity containing a photograph). For this reason, obtaining copies of identification documents certified by a suitable certifier is one of the additional verification checks that should be considered for non-face to face business.

(viii) The Code requires that a certifier shall not be relied upon unless the certifier is subject to professional rules (or equivalent) which provide the service provider with a reasonable level of comfort as to the integrity of the certifier. Suitable certifiers may include:

(a) a member of the judiciary, a senior public servant;

(b) an officer of an embassy, consulate or high commission of the country of issue of documentary evidence of identity;

(c) a lawyer or notary public who is a member of a recognised professional body;

(d) an actuary who is a member of a recognised professional body;

(e) an accountant who is a member of a recognised professional body;

(f) a notary public or equivalent

(g) a director, officer, or manager of a regulated person, or of a branch or subsidiary of a group headquartered in a well-regulated jurisdiction which applies group standards to subsidiaries and branches worldwide, and tests the application of and compliance with such standards.

(ix) The Code requires that the certifier must have provided adequate information so that he may be contacted in the event of a query. The Committee considers that this requirement would be met when the certifier include his name, position or capacity, his address

and a telephone number or email address at which he can be contacted.

(ix) A higher level of assurance will be provided where the relationship between the certifier and the person whose identity is being verified is of a professional rather than a personal nature.

Exceptions to due diligence requirements

20. Where a service provider does not apply customer due diligence measures before establishing a business relationship or carrying out an occasional transaction in reliance on regulation 16 of the Regulations, the service provider shall obtain and retain documentation establishing that regulation 16 applies.

GUIDANCE NOTES

(i) Regulation 16 of the Regulations specifies circumstances in which a service provider is not required to apply customer due diligence measures before establishing a business relationship of undertaking an occasional transaction. In summary, the exceptions apply:

(a) when the customer is a regulated person or a foreign regulated person, a company, the securities of which are listed on a recognized exchange, or a public authority in St Vincent and the Grenadines; and

(b) in respect of certain low value life insurance contracts.

These are the only exceptions. There are no other circumstances in which a service provider is not required to apply customer due diligence measures.

(ii) It is important to appreciate that the customer exceptions only apply where the customer satisfies the criteria referred to in subparagraph (a) above. They do not apply with respect to any third parties for whom the customer may be acting, or the beneficial owners of any third parties. For the purposes of the listed company exemption, the Regulations define a recognised exchange as an exchange that is a member of the World Federation of Exchanges, However, regulation 3(2) of the Regulations provides that an exchange is not a recognised exchange if it is situated in a country specified by the Committee as a country that does not implement, or does not effectively apply, the FATF Recommendations or the

Committee publishes a notice to the effect that the exchange is not a recognised exchange.

(iii) The exceptions do not apply where the service provider suspects money laundering or terrorist financing or where a higher risk of money laundering or terrorist financing has been identified.

(iv) The following may be regarded as a public authority in St Vincent and the Grenadines:

(a) the Government of St Vincent and the Grenadines;

(b) any statutory body established under a law of St Vincent and the Grenadines; and

(c) any company wholly owned by the Government of St Vincent and the Grenadines.

Intermediaries and introducers

21. (1) Before relying on an intermediary or an introducer to apply customer due diligence measures in accordance with regulation 17 of the Regulations with respect to a customer, a service provider shall:

(a) satisfy itself that the intermediary or introducer is a regulated person or a foreign regulated person and has procedures in place to undertake customer due diligence measures in accordance with, or equivalent to, the Regulations and this Code;

(b) assess the risk of relying on the intermediary or introducer with a view to determining:

(i) whether it is appropriate to rely on the intermediary or introducer; and

(ii) if it considers it is so appropriate, whether it should take any additional measures to manage that risk;

(c) where the service provider intends to rely on an introducer, obtain in writing from the introducer:

(i) confirmation that each introduced customer is an established customer of the introducer; and

(ii) sufficient information about each introduced customer to enable it to assess the risk of money

laundering and terrorist financing involving that customer; and

(d) where the service provider intends to rely on an intermediary, obtain in writing sufficient information about the customer for whom the intermediary is acting to enable the service provider to assess the risk of money laundering and terrorist financing involving that customer.

(2) A service provider shall:

(a) make and retain records:

(i) detailing the evidence that it relied upon in determining that the introducer is a regulated person, together with that evidence or copies of it, and

(ii) detailing the risk assessment carried out under subparagraph (1)(b) and any additional risk mitigation measures it considers appropriate; and

(b) retain in its records:

(i) the assurances obtained under regulation 17(2) of the Regulations and the confirmations that it has obtained under subparagraph (1)(d), and

(ii) the information that it has sought and obtained under subparagraph (1)(e).

(3) A service provider must not enter into a business relationship with a customer that is introduced by an introducer unless written terms of business are in place between the relevant person and the introducer and, those terms of business require in all cases the introducer to:

(a) verify the identity of all customers introduced to the relevant person sufficiently to comply with the AML/CFT requirements;

(b) take reasonable measures to verify the identity of the beneficial owner(s);

(c) establish and maintain a record of the evidence of identity for at least 7 years calculated in accordance with Regulation 36(1) and(2) of the Regulations;

(d) establish and maintain records of all transactions between the introducer and the customer if the records are concerned with or arise out of the introduction (whether directly or indirectly) for at least 7 years calculated in accordance with Regulation 36 (1) and (2) of the Regulations;

(e) supply to the relevant person immediately on request, copies of the evidence verifying the identity of the customer and the beneficial owner(s) and all other customer due diligence information held by the introducer in any particular case;

(f) supply to the relevant person immediately copies of theevidence verifying the identity of the customer and the beneficial owner (if any) and all other customer due diligence information, in accordance with paragraphs 8, 10, 12 or 15 (as applicable),held by the introducer in any particular case if:

(i) the introducer is to cease trading;

(ii) the introducer is to cease doing business with the customer;

(iii) the relevant person informs the introducer that it no longer intends to rely on the terms of business entered into under this paragraph;

(iv) inform the relevant person specifically of each case where the introducer is not required or has been unable to verify the identity of the customer or the beneficial owner;

(v) inform the relevant person if the introducer is no longer able to comply with the provisions of the written terms of business because of a change of the law applicable to the introducer; and

(vi) do all such things as may be required by the relevant person to enable the relevant person to comply with its obligation under sub-paragraph (8).

(4) A relevant person must ensure that the procedures under sub-paragraph (1) are fit for the purpose of ensuring that the evidence produced or to be produced is satisfactory and that the procedures of the introducer are likewise fit for that purpose.

(5) A relevant person must take measures to satisfy itself that -

(a) the procedures for implementing this paragraph are effective by testing them on a random and periodic basis no less than once every 12 months; and

(b) the written terms of business confer the necessary rights on the relevant person to satisfy the requirements of this paragraph.

(6) In order to rely upon an introducer a relevant person must:

(a) take measures to satisfy itself that the introducer is not itself reliant upon a third party for the evidence of identity of the customer in accordance with paragraphs 8, 10, 12 or 15 (as applicable); and

(b) take such measures as necessary to ensure it becomes aware of any material change to the introducer's status or the status of the jurisdiction in which the introducer is regulated.

(7) Procedures comply with this paragraph if they require, when evidence of identity in accordance with paragraphs 8, 10, 12 or 15 (as applicable) is not obtained or produced:

(a) the business relationship or occasional transaction to proceed no further; and

(b) the service provider to consider terminating that business relationship and consider making an internal disclosure according to regulation 20 of the Regulations.

(8) The ultimate responsibility for ensuring that customer due diligence procedures comply with the terms of this Code remains with the service provider and not with the introducer.

Penalty for contravening part

22. Any natural or legal person who contravenes any paragraph in this Part is guilty of an offence and is liable on summary conviction where:

(a) the person who commits the offence is a body corporate, as set out in paragraph 48 (2) and (3), it is liable to a fine of Four thousand dollars;

(b) the person who commits the offence is a partnership or an unincorporated association, as set out in paragraph 48 (4) and paragraph 48(5) respectively, it is liable to a fine of two thousand five hundred dollars; and

(c) the person who commits the offence is an individual, he is liable to a fine of one thousand five hundred dollars.

GUIDANCE NOTES

Introduction

(i) The Regulations require a service provider to determine whether a customer is acting for a third party and, if so, to:

(a) identify the third party and verify the third party's identity;

(b) to identify each beneficial owner of the third party and, taking reasonable measures on a risk-sensitive basis, to verify each of the third party's beneficial owners.

Where a customer acts for a third party, the relationship is referred to as an intermediary relationship as there is no direct relationship between the service provider and the underlying customer.

(ii) An intermediary relationship is different from an introduced relationship, as following the introduction in an introduced relationship arrangement, there is a direct relationship between the service provider and the underlying customer. The terms "intermediary" and "introducer" are defined in regulation 3(1) of the Regulations.

(iii) However, where a service provider relies on an introducer or intermediary to apply customer due diligence measures, the service provider remains liable for any failure to apply those measures.

(iv) A service provider does not have to rely on an intermediary to apply customer due diligence measures, or to apply all the customer due diligence measures. Once the business relationship is established, the service provider cannot rely on the introducer or intermediary to undertake ongoing monitoring on its behalf.

(v) The intermediary/introducer provisions do not affect arrangements whereby a service provider outsources the application of customer due diligence measures, although the service provider remains responsible for any failure.

Reliance on intermediary or introducer

(vi) In the circumstances specified in regulation 17 of the Regulations, a service provider can rely on an intermediary to apply the customer due diligence measures with respect to the customer, third parties and beneficial owners. In summary, an intermediary or introducer can be relied on if:

(a) the intermediary or introducer is a regulated person or a foreign regulated person who:

complies with the FATF requirements;

operates within a country who sufficiently applies the FATF requirements; and

does not pose a high risk for ML/TF ; and

(b) the intermediary or introducer consents to being relied on.

(vii) The Regulations expressly provide that the provisions are subject to any requirements of the Code. The Code imposes a number of additional conditions before an intermediary or introducer can be relied upon. First, a service provider must satisfy itself that the intermediary or introducer satisfies the criteria in the Regulations and then it must carry out a risk assessment to determine whether it is appropriate for it to rely on the intermediary or introducer and, if so, whether it should put in place any measures to mitigate the additional risk.

(viii)In carrying out a risk assessment, the service provider will need to consider a number of factors, including the following:

(a) the stature and regulatory track record of the intermediary or introducer;

(b) the adequacy of the framework to combat money laundering and financing of terrorism in place in the country in which the intermediary or introducer is based and the period of time that the framework has been in place;

(c) the adequacy of the supervisory regime to combat money laundering and financing of terrorism to which the intermediary or introducer is subject;

(d) the adequacy of the measures to combat money laundering and financing of terrorism in place at the intermediary or introducer;

(e) previous experience gained from existing relationships connected with the intermediary or introducer;

(f) the nature of the business conducted by the intermediary or introducer;

(g) whether relationships are conducted by the intermediary or introducer on a face to face basis;

(h) whether specific relationships are fully managed by an introducer;

(i) the extent to which the intermediary or introducer itself relies on third parties to identify its customers and to hold evidence of identity or to conduct other due diligence procedures, and if so who those third parties are; and

(j) whether or not specific intermediary or introduced relationships involve PEPs or other higher risk relationships.

(viii)Where, as a result of its risk assessment, a service provider determines that additional measures are necessary to mitigate the additional risk, these may include:

(a) making specific enquiries of the intermediary or introducer to determine the adequacy of measures to combat money laundering and financing of terrorism in place;

(b) reviewing the policies and procedures to combat money laundering and financing of terrorism in place at the intermediary or introducer;

(c) requesting specific customer due diligence information and/or copy documentation to be provided, to confirm that the intermediary or introducer is able to satisfy any requirement for such information and documentation to be available without delay at the request of the service provider; and

(d) where an intermediary or introduced relationship presents higher money laundering or financing terrorism risk, considering whether it is appropriate to rely solely upon the information provided by the intermediary or introducer, and whether additional customer due diligence information and/or documentation should be required.

(ix) Regulation 17(3) of the Regulations provides that a service provider must immediately obtain from an introducer or intermediary, the customer due diligence information concerning the customer, third party or beneficial owner. This does not extend to the evidence of identification, which must be provided to the service provider or the Committee, on its request, without delay. The phrase "without delay" means as close to immediately as possible. The Regulations and the Code do not specify a time limit because in most cases it should be possible to send electronic copies of the documents very quickly. However, even where, for good reason, it is not possible to send due diligence evidence immediately, the Committee would not accept a delay of more than 72 hours as being reasonable.

PART 3

POLICIES, PROCEDURES, SYSTEMS AND CONTROLS, RECORD KEEPING AND TRAINING

Risk assessment

23. (1) A service provider shall carry out and document a risk assessment for the purpose of:

(a) assessing the money laundering and terrorist financing risks that it faces;

(b) determining how to best manage those risks; and

(c) designing, establishing, maintaining and implementing AML/CFT policies, procedures, systems and controls that comply with the requirements of the Regulations and this Code and that are appropriate for the risks that it faces.

(2) The risk assessment carried out under subparagraph (1) shall take particular account of:

(a) the service provider's organisational structure, including the extent to which it outsources activities;

(b) the service provider's customers;

(c) the countries with which the service provider's customers are connected;

(d) the service provider's products and services; and

(e) how the service provider delivers its products and services.

(3) A service provider shall review and update the risk assessment if there are material changes to any of the matters specified in subparagraph (2).

Responsibilities of the board

24. (1) The board of a service provider has ultimate responsibility for:

(a) identifying and managing the money laundering and terrorist financing risks faced by the service provider;

(b) ensuring that adequate resources are devoted to AML/CFT efforts; and

(c) ensuring that the service provider complies with its AML/CFT obligations.

(2) Without limiting subparagraph (1), the board of a service provider has the following responsibilities:

(a) undertaking the risk assessment required by paragraph 23;

(b) on the basis of the risk assessment, establishing documented policies to prevent money laundering and terrorist financing;

(c) ensuring that:

(i) appropriate and effective AML/CFT policies, procedures, systems and controls are established, documented and implemented, and

(ii) AML/CFT responsibilities are clearly and appropriately apportioned; and

(d) assessing the effectiveness of, and compliance with, the policies, procedures, systems and controls established and promptly taking such actions as is required to remedy deficiencies.

Matters to be included in policies, procedures, systems and controls

25. (1) Without limiting regulation 20 of the Regulations, the policies, procedures, systems and controls established, maintained and implemented by a service provider under that regulation shall be documented and shall:

(a) include customer acceptance policies and procedures;

(b) provide for transaction limits and management approvals to be established for higher risk customers; and

(c) provide for the monitoring of compliance by branches and subsidiaries of the service provider both within and outside the State.

(2) A service provider shall establish, maintain and implement systems and controls and take such other measures as it considers appropriate to guard against the use of technological developments in money laundering or terrorist financing.

(3) A service provider must establish and maintain an adequately resourced and independent audit function to test compliance, including by sample testing, with the policies, procedures, systems and controls established under the Regulations and this Code.

Outsourcing

26. (1) Subject to subparagraph (2), a service provider may outsource AML/CFT activities, including obligations imposed by the Regulations or this Code.

(2) A service provider shall not outsource:

(a) its AML/CFT compliance functions;

(b) any activity, if the outsourcing of that activity would impair the ability of the service provider's supervisory authority to monitor and supervise the service provider with respect to its AML/CFT obligations;

(c) the setting and approval of its AML/CFT risk management and other strategies;

(d) oversight of its AML/CFT policies, procedures, systems and controls; or

(e) any activity unless it is satisfied that the person to whom the activity is to be outsourced will report any knowledge, suspicion, or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing activity to the service provider's AML/CFT reporting officer.

(3) A service provider shall:

(a) consider the effect that any outsourcing arrangement may have on the money laundering and terrorist financing risks that it faces; and

(b) comply with such general outsourcing requirements as may, from to time, be issued by the Committee with respect to regulated persons.

(4) Where a service provider outsources an AML or CFT activity, it retains ultimate responsibility for the performance of that activity.

Risk-sensitive approach

(i) The senior management of companies and other undertakings, both within and outside the financial sector, increasingly manage the affairs of the undertaking with regard to the risks inherent in its business and put in place systems and controls that effectively manage these risks. A risk-sensitive approach is also appropriate to managing the risks associated with money laundering and terrorist financing.

(ii) Furthermore, there are substantial differences between the various types of service providers in St Vincent and the Grenadines, and in the circumstances of different service providers of the same type, and in their customers and their customers' businesses. This diversity makes a prescriptive, and of necessity inflexible, approach to the measures required to prevent money laundering and combat terrorist financing impracticable.

(iii) International standards recognize the benefit of a risk-sensitive approach to the prevention and detection of money laundering and terrorist financing. In its June 2007 publication "Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing", the FATF states:

"By adopting a risk-based approach, competent authorities and financial institutions are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the risks identified. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention. The alternative approaches are that resources are either applied evenly, so that all financial institutions, customers, products etc. receive equal attention or that resources are targeted but on the basis of factors other than the risk assessed. This can inadvertently lead to a 'tick box' approach with the focus on meeting regulatory needs rather than combating money laundering or terrorist financing."

The AML/CFT regime therefore takes a risk-sensitive approach.

(iv) A risk-sensitive approach recognises that the money laundering and terrorist financing threat to a service provider is dependent upon a number of factors, including its customers, the countries in which it operates, the products it offers and its delivery channels and, whilst establishing minimum standards that must always be complied with, allows a service provider:

(a) to differentiate between customers in a way that matches the risk in a particular business;

(b) to apply its own approach to systems and controls and arrangements in particular circumstances; and

(c) to design more effective systems and controls that are not required to fit all circumstances.

(v) It is important to appreciate that systems and controls will not detect and prevent all money laundering or terrorist financing. A risk-sensitive approach will, however, serve to balance the cost burden placed on a service provider and its customers with a realistic assessment of the threat of the business being used in connection with money laundering or terrorist financing. It focuses the effort where it is needed and will have most impact (see the FATF publication cited above).

Risk assessment

(vi) A service provider can only fully appreciate the money laundering and terrorist financing risks that it faces by undertaking a money laundering and terrorist financing risk assessment. Paragraph 2(1) of the Code therefore requires a service provider to carry out a formal risk assessment. The risk assessment must take account of the matters specified in paragraph 2(2) of the Code.

(vii) The risk assessment will underpin the service provider's AML/CFT policies and procedures in all areas. The business of some service providers, their products and customer base may be relatively straightforward, particularly if they offer few products and their customers fall into similar categories. For these service providers, the risk assessment may enable them to design systems and controls that focus on customers that fall outside the "norm". In the case of other service providers, particularly those with

more complex products and a more diverse customer base, the systems and controls will need to be more sophisticated. The risk assessment will enable a service provider to design systems and controls that are appropriate for the risks that it faces.

(viii) Paragraph 2(1) of the Code requires the risk assessment to be documented. When undertaking on-site compliance visits, as part of its assessment of a service provider, the supervisory authority will require documented evidence that a money laundering and terrorist financing risk assessment has been undertaken.

(ix) The money laundering and terrorist financing risk assessment should be kept under regular review and updated as necessary, particularly if there are material changes in the service provider's business or customers or the risks that it faces. It is not possible to say how often a formal reassessment will be required as this will depend upon the circumstances of a particular service provider. For some service providers it may be appropriate for a reassessment to be carried out annually. However, for many service providers, particularly those with a relatively stable business and customer base, the reassessment would not need to be undertaken so frequently.

(x) The risk assessment is only the first part of implementing a risk-sensitive approach. Building on the risk assessment, a service provider should prepare a risk profile for each customer, which will build up over time, allowing the service provider to identify transactions or activities that may be suspicious. This is covered further in the following paragraphs of the Code.

Responsibilities of board

(xi) The principal responsibilities of the board are set out in paragraph 2 of the Code. The Board will be assisted in fulfilling these responsibilities by the AML/CFT reporting officer, the AML/CFT compliance officer and senior management. Larger or more complex service providers may also require dedicated risk and internal audit functions to assist in the assessment and management of money laundering and terrorist financing risk.

Policies, systems and controls

(xii) Regulation 20 of the Regulations sets out broad requirements with respect to the risk-sensitive money laundering and terrorist financing policies, procedures, systems and controls that must be established, maintained and implemented by a service provider. The matters required to be covered by the AML/CFT policies, procedures, systems and controls include the following:

(a) customer due diligence measures and ongoing monitoring;

(b) the reporting of suspicious activities;

(c) record-keeping;

(d) screening of employees;

(e) internal controls;

(f) risk assessment and management;

(g) the monitoring and management of compliance;

(h) the internal communication of its policies, procedures, systems and controls;

(i) the identification and scrutiny of:

(I) the background of complex or unusually large transactions;

(II) the background of unusual patterns of transactions which have no apparent economic or visible lawful purpose; and

(III) any other activity which the service provider regards as particularly likely by its nature to be related to the risk of money laundering or terrorist financing;

As far as possible and document all findings in writing.

(j) the taking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products and transactions which are susceptible to anonymity.

These are supplemented by paragraph 2 of the Code. To be effective, the AML/CFT systems and controls must be appropriate given the circumstances of a particular service provider.

(xiii) Paragraph 2(2)(d) of the Code provides that the board has responsibility for assessing the effectiveness of, and compliance with, the policies, procedures, systems and controls established and promptly taking such actions as is required to remedy deficiencies.

(xiv) In order to assess the effectiveness of the AML/CFT policies, procedures, systems and controls, the board will need, amongst other things, to:

(a) ensure that it receives regular, timely and adequate information relevant to the management of the service provider's money laundering and terrorist financing risk;

(b) monitor the ongoing competence and effectiveness of the AML/CFT reporting officer and the AML/CFT compliance officer;

(c) undertake periodic reviews of the adequacy of policies and procedures for higher risk customers;

(d) consider whether the incidence of suspicious activity reports (or an absence of such reports) has highlighted any deficiencies in the service provider's customer due diligence or reporting policies and procedures and whether changes are required to address any such deficiencies;

(e) consider whether inquiries have been made by the Financial Intelligence Unit, or production orders received, without issues having previously being identified by customer due diligence or reporting policies and procedures;

(f) consider changes made or proposed in respect of new legislation, regulatory requirements or guidance, or as a result of changes in business activities.

(xv) In order to assess compliance with the AML/CFT policies, procedures, systems and controls, the board will need to periodically commission and consider a compliance report from the AML/CFT compliance officer.

(xvi) Paragraph 2(1) of the Code provides that the policies, procedures, systems and controls must be documented. Part of this documentation usually includes a procedures manual, which may be paper-based or electronic. A comprehensive procedures manual is an excellent ongoing reference source for employees and others, and may also be useful for staff training. The procedures manual must be written or tailored for the service provider and its particular circumstances. It is not, therefore, appropriate for the Code to specify a format for or the contents of the procedures manual. However, by way of guidance only, the procedures manual should normally include the issues and matters set out in the Schedule to the Code.

(xvii) Paragraph 2(3) of the Code requires a service provider to establish and maintain an adequately resourced and independent audit function to test compliance with its AML/CFT policies, procedures, systems and controls. This function should be undertaken by a service provider's internal audit function, if it has one. If a service provider does not have an internal audit function, this function may be outsourced under an outsourcing agreement, provided that the person to whom the function has been outsourced is independent and adequately resourced.

Outsourcing

(xviii) Paragraph 2(2) of the Code provides that a service provider must not outsource its AML/CFT compliance function. This means that a service provider may not outsource the compliance function as a whole. However, where appropriate, a service provider may outsource certain specific compliance activities.

Ongoing monitoring policies, procedures, systems and controls

27. (1) The ongoing monitoring policies, procedures, systems and controls established by a service provider in accordance with regulation 20 of the Regulations shall:

(a) provide for a more thorough scrutiny of higher risk customers;

(b) be designed to identify unusual and higher risk activity or transactions and require that special attention is paid to higher risk activity and transactions;

(c) require that any unusual or higher risk activity or transaction is examined by an appropriate person to determine the background and purpose of the activity or transaction;

(d) require the collection of appropriate additional information;

(e) be designed to establish whether there is a rational explanation, an apparent economic or visible lawful purpose, for unusual or higher risk activity or transactions identified, and require a written record to be kept of the service provider's conclusions.

(2) When conducting ongoing monitoring, a service provider shall regard the following as presenting a higher risk:

(a) complex transactions;

(b) unusual large transactions;

(c) unusual patterns of transactions, which have no apparent economic or lawful purpose;

(d) activity and transactions:

(i) connected with countries which do not, or insufficiently apply, the FATF Recommendations; or

(ii) which are the subject of United Nations or European Union countermeasures; and

(e) activity and transactions that may be conducted with persons who are the subject of United Nations or European Union sanctions and measures.

Penalty for contravening part

28. Any natural or legal person who contravenes any paragraph in this Part is guilty of an offence and is liable on summary conviction where:

(a) the person who commits the offence is a body corporate, as set out in paragraph 48 (2) and (3) it is liable to a fine of four thousand dollars;

(b) the person who commits the offence is a partnership or an unincorporated association, as set out in paragraph 48 (4) and paragraph 48(5) respectively, it is liable to a fine of two thousand five hundred dollars; and

(c) the person who commits the offence is an individual, he is liable to a fine of one thousand five hundred dollars.

GUIDANCE NOTES

Requirements of the Regulations concerning ongoing monitoring

(i) Regulation 11(5) of the Regulations require a service provider to undertake ongoing monitoring of a business relationship. Ongoing monitoring is defined in regulation 7 of the Regulations as:

(a) scrutinising transactions undertaken throughout the course of the relationship, including where necessary the source of funds, to ensure that the transactions are consistent with the service provider's knowledge of the customer and his business and risk profile; and

(b) keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date and relevant by undertaking reviews of existing records.

(ii) Paragraph 2(1) of the Code requires a service provider to have policies systems and controls relating to ongoing monitoring that which provide for, amongst other things:

(a) the identification and scrutiny of:

(I) complex or unusually large transactions;

(II) unusual patterns of transactions which have no apparent economic or visible lawful purpose; and

(III) any other activity which the service provider regards as particularly likely by its nature to be related to the risk of money laundering or terrorist financing; and

(b) determining whether:

(I) a customer, any third party for whom the customer is acting and any beneficial owner of the customer or third party, is a politically exposed person;

(II) a business relationship or transaction, or proposed business relationship or transaction, is with a person connected with a country that does not apply, or insufficiently applies, the FATF Recommendations;

(III) a business relationship or transaction, or proposed business relationship or transaction, is with a person connected with a country or territory that is subject to measures for purposes connected with the prevention and detection of money laundering or terrorist financing, imposed by one or more countries or sanctioned by the European Union or the United Nations.

(iii) Regulation 14(2) of the Regulations requires a service provider to undertake enhanced ongoing monitoring in the same circumstances as enhanced customer due diligence measures are require to be applied, ie:

(a) where the customer has not been physically present for identification purposes;

(b) where the service provider has, or proposes to have, a business relationship with, or proposes to carry out an occasional transaction with, a person connected with a country or territory that does not apply, or insufficiently applies, the FATF Recommendations;

(c) where the service provider is a SVG bank that has or proposes to have a banking or similar relationship with an institution whose address for that purpose is outside St Vincent and the Grenadines;

(d) where the service provider has or proposes to have a business relationship with, or to carry out an occasional transaction with, a politically exposed person;

(e) where any of the following is a politically exposed person:

(I) a beneficial owner of the customer;

(II) a third party for whom a customer is acting;

(III) a beneficial owner of a third party described in subparagraph (ii);

(IV) a person acting, or purporting to act, on behalf of the customer; and

(f) in any other situation which by its nature can present a higher risk of money laundering or terrorist financing.

Undertaking ongoing monitoring

(iv) The principal objective of ongoing monitoring is to identify higher risk activity and business relationships so that money laundering and terrorist financing can be identified and, if possible, prevented.

(v) The essentials of any monitoring systems and controls are that:

(a) they flag transactions and/or activities for further examination;

(b) ongoing monitoring reports are reviewed promptly by the right person(s); and

(c) appropriate action is taken on the findings of any further examination.

(vi) Monitoring can either take place:

(a) as transactions and/or activities take place or are about to take place, or

(b) after the event, through some independent review of the transactions and/or activities that a customer has undertaken,

and in either case, unusual transactions or activities must be flagged for further examination.

(vii) Monitoring may be by reference to specific types of transactions, to the profile of the customer, or by comparing their activity or profile with that of a similar peer group of customers or through a combination of these approaches.

(viii) A service provider should also have systems and procedures to deal with customers who have not had contact with it for some time, in circumstances where regular contact might be expected, and with dormant accounts or relationships, to be able to identify future reactivation and unauthorized use.

(ix) In designing monitoring systems and controls, it is important that appropriate account is taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer and product risk.

(x) Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. Nevertheless, where a service provider has a substantial number of customers with a high level of transactions, an automated monitoring system may be effective. However, use of an automated monitoring system does not remove the requirement for a service provider to remain vigilant to the risk of money laundering or terrorist financing.

PART 4

COMPLIANCE AND REPORTING OBLIGATIONS

Reporting procedures

29. (1) A service provider shall establish and maintain reporting procedures that:

(a) communicate the identity of the AML/CFT reporting officer to its employees;

(b) require that a report is made to the AML/CFT reporting officer of any information or other matter coming to the attention of any employee handling relevant business which, in the opinion of that person, gives rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering or terrorist financing;

(c) require that a report is considered promptly by the AML/CFT reporting officer in the light of all other relevant information for the purpose of determining whether or not the information or other matter contained in the report gives rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing;

(d) allow the AML/CFT reporting officer to have access to all other information which may be of assistance in considering the report;

(e) require the information or other matter contained in a report to be disclosed as soon as is reasonably practicable by the AML/CFT reporting officer to the Financial Intelligence Unit in writing, where the AML/CFT reporting officer knows, suspects or has reasonable grounds to know or suspect that another person is engaged in money laundering or terrorist financing; and

(f) require the AML/CFT reporting officer to report to the Financial Intelligence Unit attempted transactions and business that have been refused (regardless of the amount of the attempted transaction or the value of the refused business), where the attempted transaction or refused business gives rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing.

(2) For the purposes of this paragraph, AML/CFT reporting officer includes any deputy AML/CFT reporting officer that may be appointed.

Internal reporting procedures

30. (1) A service provider shall establish internal reporting procedures that require:

(a) that, where a customer fails to supply adequate customer due diligence information, or adequate documentation verifying identity (including the identity of any beneficial owners), consideration should given to making a suspicious activity report;

(b) the reporting of attempted transactions and business that has been refused, regardless of the amount of the attempted transaction or the value of the refused business, where the attempted transaction or refused business gives rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing;

(c) employees to make internal suspicious activity reports containing all relevant information in writing to the

AML/CFT reporting officer as soon as it is reasonably practicable after the information comes to their attention;

(d) suspicious activity reports to include as full a statement as possible of the information giving rise to knowledge or reasonable grounds for suspicion of money laundering or terrorist financing activity and full details of the customer;

(e) that reports are not filtered out by supervisory staff or managers so that they do not reach the AML/CFT reporting officer;

(f) suspicious activity reports to be acknowledged by the AML/CFT reporting officer.

(2) A service provider shall establish and maintain arrangements for disciplining any employee who fails, without reasonable excuse, to make an internal suspicious activity report where he or she has knowledge or reasonable grounds for suspicion of money laundering or terrorist financing.

Evaluation of suspicious activity reports

31. A service provider shall ensure that:

(a) all relevant information is promptly made available to the AML/CFT reporting officer on request so that internal suspicious activity reports are properly assessed;

(b) each suspicious activity report is considered by the AML/CFT reporting officer in light of all relevant information; and

(c) the AML/CFT reporting officer documents the evaluation process followed and reasons for the decision to make a report or not to make a report to the Financial Intelligence Unit.

Reports to Financial Intelligence Unit

32. (1) A service provider shall require the AML/CFT reporting officer to make external suspicious activity reports directly to the Financial Intelligence Unit as soon as practical, and in any event within 14 days after the information or other matter comes to the AML/CFT compliance officer's attention, that:

(a) include the information specified in subparagraph (2); and

(b) are in such form as may be prescribed or specified by the Financial Intelligence Unit.

(2) The information required to be included in a report to the Financial Intelligence Unit for the purposes of subparagraph (1) is:

(a) full details of the customer and as full a statement as possible of the information giving rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion;

(b) if a particular type of criminal conduct is suspected, a statement of this conduct;

(c) where a service provider has additional relevant evidence that could be made available, the nature of this evidence; and

(d) such statistical information as the Financial Intelligence Unit may require.

(3) The AML/CFT compliance officer of a service provider shall, on or before March 31st of each calendar year, submit an annual compliance report to the Financial Intelligence Unit in such form and containing such information as it may specify.

(4) The AML/CFT compliance officer of a service provider shall file quarterly reports to the supervisory authority, in such form and containing such information as the Financial Intelligence Unit shall specify, specifying the number of suspicious activity reports, submitted to the Financial Intelligence Unit in the quarter.

(5) The quarterly reports shall be filed as follows:

(a) a report for the quarter ended 31st March shall be submitted to the supervisory authority on or before 10th April;

(b) a report for the quarter ended 30th June shall be submitted to the supervisory authority on or before 10th July;

(c) a report for the quarter ended 30th September shall be submitted to the supervisory authority on or before 10th October; and

(d) a report for the quarter ended 31st December shall be submitted to the supervisory authority on or before 10th January of the following year.

(6) A natural or legal person who fails to submit annual compliance reports and quarterly reports to the Financial Intelligence Unit in accordance with this paragraph is guilty of an offence and is liable on summary conviction to a fine where:

(a) the person who commits the offence is a body corporate, as set out in paragraph 48 (2) and (3) it is liable to a fine of four thousand dollars;

(b) the person who commits the offence is a partnership or an unincorporated association, as set out in paragraph 48 (4) and paragraph 48 (5) respectively, it is liable to a fine of two thousand five hundred dollars; and

(c) the person who commits the offence is an individual, he is liable to a fine of one thousand five hundred dollars.

Guidance Notes

AML/CFT reporting officer

(i) Regulation 25 of the Regulations requires every service provider to appoint a AML/CFT reporting officer. The AML/CFT reporting officer has responsibility for receiving internal money laundering disclosures, deciding whether these disclosures should be reported to the Financial Intelligence Unit and, if he so decides, making the reports to the Financial Intelligence Unit, and acting as the liaison point with the Financial Intelligence Unit and a service provider's supervisory authority.

(ii) A service provider with a substantial business may need to appoint other individuals to assist the AML/CFT reporting officer. Where such other individuals are appointed, it is permissible for its procedures to permit employees to make internal reports to these

individuals, on behalf of the AML/CFT reporting officer. However, the AML/CFT reporting officer has ultimate responsibility for all reports made by employees of the service provider and any other individuals appointed must be answerable to the AML/CFT reporting officer.

(iii) The AML/CFT reporting officer will have more knowledge and experience relevant to the prevention of money laundering and terrorist financing than other employees of the service provider. The Regulations anticipate that the AML/CFT reporting officer will use his knowledge and experience to fully assess the disclosure that has been made to him and that he will only make a suspicious activity report to the Financial Intelligence Unit if he considers, after his assessment, that the information disclosed gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of money laundering or terrorist financing. The AML/CFT reporting officer is expected to act as a filter and not to routinely pass all disclosures made to him to the Financial Intelligence Unit without making his own assessment.

(iv) Where the size of the service provider's business permits, the AML/CFT reporting officer may carry on other functions within the service provider, provided that they do not conflict with his duties as AML/CFT reporting officer.

(v) The AML/CFT reporting officer must:

(a) oversee any deputy AML/CFT reporting officer or other staff appointed to assist him; and

(b) maintain full and clear records of all disclosures that he has received and all suspicious activity reports he has made.

(vi) The AML/CFT reporting officer must also take great care to manage relationships with clients appropriately to avoid tipping off any third parties.

AML/CFT compliance officer

(vii) Regulation 25 of the Regulations also requires every service provider to appoint a AML/CFT compliance officer. The AML/CFT compliance officer can be the same person as the AML/CFT reporting officer and, in the case of a regulated person, can be the

same person as the person appointed as compliance officer for the purposes of regulatory compliance, if approved by the relevant supervisory authority.

(viii) However, a regulated person may split the reporting and compliance functions and appoint different individuals as its AML/CFT reporting officer and AML/CFT compliance officer.

Disclosure requirements

(ix) The Act and the Anti-Terrorist Financing and Proliferation Act contain disclosure requirements concerning knowledge or suspicion (or grounds for knowledge or suspicion) of money laundering or terrorist financing. Part 4 of the Code, and the Guidance Notes that follows, is designed to outline and amplify the statutory disclosure requirements. The obligations to disclose are so important that they are set out in detail in the Guidance Notes.

Statutory requirements

(x) Section 126 of the Act and Section 15 of the Anti-Terrorist Financing and Proliferation Act requires a person to make a disclosure to the Financial Intelligence Unit or the person's AML/CFT reporting officer if the person:

(a) knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering or has committed or attempted to commit a terrorist financing offence; and

(b) the information or other matter on which the person's knowledge or suspicion is based, or which gives reasonable grounds for such knowledge or suspicion, came to him in the course of a relevant business.

The information or other matter must be disclosed as soon as is practicable after it comes to him.

(xi) It is beyond the scope of the Guidance Notes to consider the money laundering and terrorist financing offences themselves:

(a) concealing, disguising, converting, transferring and removing criminal property;

(b) entering into or becoming concerned in an arrangement which a person knows or suspects facilitates, by whatever means, the acquisition, retention, use or control of criminal property by or on behalf of another person; and

(c) acquisition, use or possession of criminal property.

It is essential that every service provider provides relevant staff with training concerning the money laundering and terrorist financing offences.

(xii) Relevant business is the business of a service provider. In the circumstances, the obligation to disclose is imposed on any person where the information came to that person "in the course of the relevant business". The disclosure requirements therefore apply to the service provider itself as well as directors and all employees of a service provider. The knowledge or suspicion may relate to any person, including the service provider itself. Therefore, if a service provider (or one of its employees) believes that the service provider may have, itself, committed a money laundering or terrorist financing offence, for example by becoming concerned in an arrangement facilitating money laundering or terrorist financing, a report must be made.

(xiii) All service providers are required by the Regulations to establish procedures for making disclosures. This applies both to internal reports, ie disclosure reports within the service provider to the AML/CFT reporting officer and external reports, ie disclosure reports to the Financial Intelligence Unit. An employee is expected to make a suspicious activity report (SAR) in accordance with the employer's internal reporting procedures, not directly to the Financial Intelligence Unit. Provided an employee does this, the employee will not commit an offence under section 126 of the Act.

(xiv) The effect of section 126 of the Act and ***Section 15 of the Anti-Terrorist Financing and Proliferation Act*** *is to require that the disclosure must be made before any actions are taken with respect to the business relationship or occasional transaction concerned, unless:*

(a) the service provider has the consent, or the deemed consent, of the Financial Intelligence Unit; or

(b) the person who takes the action had good reason for his failure to make the disclosure before he took action concerning the business relationship or occasional transaction and the disclosure is made on his own initiative and as soon as it is practicable for him to make it afterwards.

(xv) A person who fails to make a report when required to do so, in accordance with section 126 ***of the Act and Section 15 of the Anti-Terrorist Financing and Proliferation Act****, commits an offence. As indicated above, an offence may be committed not just by the service provider but also by its employees.*

Offences involving or relating to tax

(xvi) Criminal conduct is defined in the Act as "conduct which constitutes an offence or would constitute an offence if it had occurred in the State". For this purpose, "offence" is defined as an offence that may be proceeded with on indictment or that, where it may only be tried summarily, the maximum penalty in the case of an individual would be a term of imprisonment of 1 year or more.

(xvii) Furthermore, offences under the Customs (Control and Management) Act are scheduled offences for the purposes of section 16(1) (a) of the Act (Schedule 7).

(xviii) There are no exceptions to the definition of "offence" in relation to tax, or any other, matters. Therefore, an offence, within the Act definition, that involves or relates to tax is as capable of constituting criminal conduct as any other type of offence.

(xix) In the circumstances, service providers and their employees are obliged to report any knowledge, suspicion or reasonable grounds for knowledge or suspicion of money laundering, even though the predicate offence may be a tax offence or may involve or relate to tax, and their reporting procedures should reflect this.

PART 5

EMPLOYEE TRAINING AND AWARENESS AND RECORD KEEPING

Training and vetting obligations

33. (1) A service provider shall:

(a) provide appropriate basic AML/CFT awareness training to employees whose duties do not relate to the provision of relevant business;

(b) establish and maintain procedures that monitor and test the effectiveness of its employees' AML/CFT awareness and the training provided to them;

(c) vet the competence and probity of employees whose duties relate to the provision of relevant business at the time of their recruitment and at any subsequent change in role and ensure that their competence and probity is subject to ongoing monitoring;

(d) provide training, to temporary and contract staff and, where appropriate, the staff of any third parties fulfilling a function in relation to a service provider under an outsourcing agreement; and

(e) provide employees with adequate training in the recognition and handling of transactions at appropriate frequencies.

(2) The training provided by a service provider shall:

(a) be tailored to the business carried out by the service provider and relevant to the employees to whom it is delivered, including particular vulnerabilities of the service provider;

(b) be conducted with the appropriate level of detail to ensure a good understanding and appreciation of the issues relative to money laundering and terrorist financing;

(a) be designed to test employee knowledge of anti-money laundering and terrorist financing issues commensurate with established standards;

(c) explain the meaning of "money laundering" for the purposes of the Act, the Regulations and this Code and the meaning of "terrorist financing", cover the legal obligations of employees to make disclosures under section 126 of the Act and **section 15 of the Anti-Terrorist Financing and Proliferation Act** and explain the circumstances in which such disclosures are required to be made;

(d) pertain to the familiarization with the provisions of the laws (list laws) and attending regulations, the reporting entity's internal compliance procedures and with international standards stemming from the international money laundering and terrorist financing prevention conventions, and with the guidelines.

(c) explain the risk-based approach in the prevention and detection of money laundering and terrorist financing focusing but not limited to areas such as wire transfer, credit card, money remittances services and correspondent accounts.

(d) highlight to employees the importance of the contribution that they can individually make to the prevention and detection of money laundering and terrorist financing; and

(e) be provided to employees as soon as practicable after their appointment and periodically using a risk based approach.

Penalty

34. A service provider who contravenes paragraph 33 is guilty of an offence and is liable on summary conviction to a fine of three thousand dollars.

GUIDANCE NOTES

Introduction

(i) The staff of a service provider, as its "eyes and ears", are crucial to its efforts to prevent the service provider being used for the purposes of money laundering or terrorist financing. However, unless those employees that have access to information which

may be relevant in determining whether any person is engaged in money laundering or terrorist financing are properly trained and understand how to recognize suspicious transactions and activities, they will not be in a position to fulfil this vital role.

(ii) The employees of a service provider must also understand and be able to apply the procedures, systems and controls that a service provider has put in place to prevent and detect money laundering and terrorist financing. If staff do not apply the procedures, systems and controls properly, they will not be effective, however well designed they may be. In particular, it is important that staff understand the risk-sensitive approach to the prevention of money laundering and terrorist financing.

(iii) It is, of course, also vital that staff are honest. One dishonest member of staff could cause substantial problems for a service provider. Put simply, the staff of a service provider may be either its greatest asset or its greatest liability in its efforts to prevent it being used for money laundering and terrorist financing.

(iv) The training of employees may take different forms –

internal workshops or seminars provided by the entity or professional, a domestic industry-organized training, overseas training, etc. Whatever formula is adopted, it is imperative that the requirements of Regulation 24 are complied with and the necessary record keeping requirements outlined in Part VII of this Code are complied with

(iv) It is for these reasons that the Regulations and the Code contain a number of requirements concerning staff training and awareness.

Statutory requirements

(v) Regulation 24(1) of the Regulations requires service providers to take appropriate measures for the purposes of making employees whose duties relate to the provision of relevant business aware of:

(a) the anti-money laundering and counter-terrorist financing policies, procedures, systems and controls maintained by the service provider in accordance with these Regulations and the Code;

(b) the law of the State relating to money laundering and terrorist financing offences; and

(c) the Regulations, the Code and any Guidance Guidance issued by the Committee

(vi) Regulation 24(2) requires service providers to provide employees referred to in paragraph (v) with training in the recognition and handling of:

(a) transactions carried out by or on behalf of any person who is or appears to be engaged in money laundering or terrorist financing; and

(b) other conduct that indicates that a person is or appears to be engaged in money laundering or terrorist financing.

(vii) Training is required to include the provision of information on current money laundering ***and terrorist financing*** *techniques, methods, trends and typologies.*

(viii) The requirements of the Regulations are supplemented by the Code.

Employees whose duties relate to the provision of relevant business

(ix) The principal training obligations are in respect of employees whose duties relate to the provision of relevant business. When considering whether an employee falls within this criterion, a service provider should take the following into account:

(a) whether the employee is undertaking any customer facing functions, or handles or is responsible for the handling of business relationships or transactions;

(b) whether the employee is directly supporting a colleague who carries out the above activity; and

(c) whether an employee's role has changed to involve the above activities.

(x) The directors and senior managers of a service provider should always be considered to fall within the criterion, whatever their roles.

Vetting of relevant employees

(xi) The Code requires a service provider to vet the competence and probity of employees whose duties relate to the provision of relevant business at the time of their recruitment and at any subsequent change in role and that their competence and probity is subject to ongoing monitoring. As discussed above, it is vital that employees are honest: The most effective way of achieving this is for the service provider to vet and then to monitor its employees, particularly those subject to this requirement for competence and probity.

(xii) Whilst the most appropriate methods for vetting and monitoring employees is a matter for the judgment of each service provider, there are a number of obvious steps that may be taken, including:

(a) obtaining and confirming references with respect to prospective new employees;

(b) confirming the employment history and qualifications of prospective new employees;

(c) requesting and verifying details of any regulatory action taken against the employee concerned;

(d) requesting and verifying details of any criminal convictions.

Staff Awareness

(xiii) The requirements of the Regulations cover awareness and training. As indicated above, it is a statutory requirement that a service provider takes appropriate measures for the purpose of making all relevant employees aware of the Act, the Anti-Terrorist financing and Proliferation Act, the Regulations, any applicable Code and any Guidance issued by the Committee or a relevant supervisory body and the AML/CFT policies, procedures, systems and controls maintained by the service provider.

(xiv) In order to demonstrate compliance with the Regulations, a service provider will need to have measures in place to make employees aware of:

(a) the AML/CFT procedures, systems and controls in place to prevent and detect money laundering and terrorist financing;

(b) employees' potential personal liability [criminal, regulatory and disciplinary] for breaches of the statutory provisions and in particular for any failure to make a disclosure as required by section 126 of the Act and Section 17 of the Anti-Terrorist financing and Proliferation Act;

(c) the potential implications to the service provider for any breaches of the Act, the Anti-Terrorist financing and Proliferation Act, the Regulations and any applicable Code.

(xv) The design of appropriate awareness measures is a matter for each service provider to determine. However, such measures would usually include:

(a) providing relevant employees with a copy of the AML/CFT procedures manual;

(b) providing relevant employees with a document outlining the service provider's and their own obligations and potential criminal liability under the Act, the Anti-Terrorist financing and Proliferation Act, the Regulations and the Code;

(c) requiring employees to acknowledge that they have received and understood the AML/CFT procedures manual and the document outlining statutory obligations; and

(d) periodically testing employees' awareness of policies and procedures and statutory obligations.

(xvi)It should be noted that it is not sufficient simply to provide employees with copies of the Act, the Anti-Terrorist Financing and Proliferation Act, the Regulations and any applicable Codes. Given the risk-sensitive approach adopted by the St Vincent and the Grenadines regime, every service provider will need to put in place its own systems and controls and procedures that are appropriate for its business.

(xvii)Paragraph 3(1) (a) of the Code requires basic AML/CFT awareness training to be provided to employees whose duties do

not relate to the provision of relevant business. This will usually require the service provider, at a minimum to:

(a) inform employees of the identity of the AML/CFT reporting officer and the procedures to make internal suspicious activity reports;

(b) provide employees with a document outlining the service provider's and their own obligations and potential criminal liability under the Act, the Anti-Terrorist Financing and Proliferation Act and the Regulations and providing some basic information concerning the Code; and

(c) require employees to acknowledge that they have received and understood the procedures for making internal suspicious activity reports and the document outlining statutory obligations.

(xviii) One-off awareness training should not be considered to be sufficient. It is important that staff, particularly employees whose duties relate to the provision of relevant business, are kept up to date with AML/CFT developments both in St Vincent and the Grenadines and internationally.

Staff training

(xix) The Regulations require that a service provider must provide all employees whose duties relate to the provision of relevant business with appropriate training in the recognition and handling of transactions carried out by or on behalf of any person who is, or appears to be, engaged in money laundering or terrorist financing. In order to demonstrate compliance with this, a service provider should consider including within its training to relevant employees training on:

(a) the recognition and handling of unusual, complex, or higher risk activity and transactions, such as activity outside of the expected patterns, unusual settlements, abnormal payment or delivery instructions and changes in the patterns of business relationships; some areas of focus may include transactions relating to credit card operations, correspondent banking, wire transfers and frequent loans.

(b) money laundering and terrorist financing trends and typologies;

management of customer relationships which have been the subject of a suspicious activity report, e.g. risk of committing the offence of tipping off, and dealing with questions from such customers, and/or their adviser;.

Paragraph 3(2) (b) of the Code provides that the training should explain the meaning of the terms "money laundering" and terrorist financing. A service provider should ensure, in particular, that the training it provides enables employees to understand the linkages between "money laundering" and the proceeds of crime so that they fully understand that the disclosure requirement imposed by section 126 of the Act includes a requirement to make a disclosure whenever an employee knows or suspects, or has reasonable grounds for knowing or suspecting, that funds are the proceeds of crime.

A service provider should ensure, in particular, that the training it provides enables employees to understand that the disclosure requirement imposed by section 17 of the Anti-Terrorist Financing and Proliferation Act includes a requirement to make a disclosure whenever an employee knows or suspects, or has reasonable grounds for knowing or suspecting, that another person has committed or attempted to commit a terrorist financing offence.

(xxi) Paragraph 3(1)(d) of the Code requires a service provider to provide training, where appropriate, to the staff of any third parties fulfilling a function in relation to a service provider under an outsourcing agreement. A service provider should not enter into an outsourcing agreement with a third party unless it is satisfied that the third party is suitably qualified and knowledgeable to undertake the outsourced work. The Committee does not, therefore, expect that a service provider will need to provide basic money laundering training to the staff of third parties. However, some training may be appropriate. For example, staff of the third party may require training concerning the specific AML/CFT procedures of the service provider or concerning the specific AML/CFT risks that the service provider faces.

Monitoring the effectiveness of AML/CFT training

(xxii) Monitoring the effectiveness of AML/CFT training will usually require:

(a) periodic testing of employees' understanding of the service provider's AML/CFT policies, procedures, systems and controls and their ability to recognise money laundering and terrorist financing activity;

(b) monitoring the compliance of employees with the AML/CFT systems and controls; and

(c) monitoring internal reporting patterns.

Meaning of "records"

35. In this Part "records" means records that a service provider is required to keep by the Regulations or this Code.

Minimum retention period

36. (1) Subject to subparagraph (2), the minimum period for the retention of records for the purposes of this Code and the Regulations is 7 years.

(2) The service provider's supervisory authority or the Financial Intelligence Unit may, by written notice, specify a period longer than 7 years for the purposes of subparagraph (1), and such longer period as is specified in the notice shall be considered to be the minimum retention period instead of the period of 7 years.

Transaction records

37. (1) Records relating to transactions with customers shall contain the following information concerning each transaction carried out:

(a) the name and address of the customer;

(b) if the transaction is a monetary transaction, the currency and the amount of the transaction;

(c) if the transaction involves a customer's account, the number, name or other identifier for the account;

(d) the date of the transaction;

(e) details of the counterparty, including account details;

(f) the nature of the transaction; and

(g) details of the transaction.

(2) A service provider shall, together with its records concerning a business relationship or occasional transaction, keep for

the minimum retention period, all customer files and business correspondence relating to the relationship or occasional transaction.

(3) The transaction records kept by a service provider shall:

(a) contain sufficient details to enable a transaction to be understood; and

(b) enable an audit trail of the movements of incoming and outgoing funds or asset movements to be readily constructed.

Records concerning suspicious activities etc

38. (1) A service provider shall keep for a period of 7 years from the date a business relationship ends, or for 7 years from the date that an occasional transaction was completed, records containing, with respect to that business relationship or transaction:

(a) any internal suspicious activity reports and supporting documentation;

(b) the decision of the AML/CFT reporting officer concerning whether to make a suspicious activity report to the Financial Intelligence Unit and the basis of that decision;

(c) details of any reports made to the Financial Intelligence Unit; and

(d) records concerning reviews of:

(i) complex transactions,

(ii) unusual large transactions,

(iii) unusual patterns of transactions, which have no apparent economic or visible lawful purpose, and

(iv) customers and transactions connected with countries which do not apply, or insufficiently apply, the FATF Recommendations or are the subject of United Nations or European Union countermeasures.

(2) A service provider shall keep records of all enquiries relating to money laundering or terrorist financing made to it by the Financial

Intelligence Unit for a period of at least 7 years from the date that the enquiry was made.

Records concerning policies, systems and controls and training

39. (1) A service provider shall keep records documenting its policies, systems and controls to prevent and detect money laundering for a period of at least 7 years from the date that the policies, systems and controls are superseded or otherwise cease to have effect.

(2) A service provider shall keep records for at least 7 years detailing all dates on which training on the prevention and detection of money laundering and the financing of terrorism was provided to employees, the nature of the training and the names of employees who received the training.

Outsourcing

40. (1) If a service provider outsources record keeping to a third party, the service provider remains responsible for compliance with the record keeping requirements of the Regulations and this Code.

(2) A service provider shall not enter into outsourcing arrangements or place reliance on third parties to keep records where access to records is likely to be impeded by confidentiality or data protection restrictions.

Reviews of record keeping procedures

41. A service provider shall:

(a) periodically review the accessibility of, and condition of, paper and electronically retrievable records and consider the adequacy of the safekeeping of records; and

(b) periodically test procedures relating to the retrieval of records.

Penalty

42. A service provider who contravenes paragraphs 34 to 39 is guilty of an offence and is liable on summary conviction to a fine where:

(a) the person who commits the offence is a body corporate, as set out in paragraph 48 (2) and (3) it is liable to a fine of one thousand dollars;

(b) the person who commits the offence is a partnership or an unincorporated association, as set out in paragraph 48 (4) and paragraph 48 (5) respectively, it is liable to a fine of seventy five thousand dollars; and

(c) the person who commits the offence is an individual, he is liable to a fine of thirty thousand dollars.

GUIDANCE NOTES

Introduction

(i) The principal reason for imposing record keeping requirements on service providers is to ensure that the law enforcement agencies in St Vincent and the Grenadines are not prevented from investigating and prosecuting money laundering and terrorist financing offences and investigating claims for the confiscation of the proceeds of crime and from assisting overseas law enforcement agencies in their investigations and prosecutions.

If law enforcement agencies, either in St Vincent and the Grenadines or elsewhere, are unable to trace criminal property due to inadequate record keeping, then prosecution for money laundering, terrorist financing and the confiscation of criminal property may not be possible. If the funds used to finance terrorist activity cannot be traced back through the financial system, it will not be possible to identify the sources and the destination of terrorist funding.

(ii) The Regulations therefore impose certain record keeping requirements on service providers. These are summarized in the following paragraphs.

(iii) Service providers are required to keep:

(a) copies of evidence of identity, or information that enables a copy of the evidence to be obtained;

(b) the supporting documents, data or information that have been obtained in respect of a business relationship or occasional transaction, which must include sufficient information to enable the reconstruction of individual transactions;

(c) a record containing details relating to each transaction carried out by the service provider in the course of any business relationship or occasional transaction.

(iv) Records relating to transactions must include sufficient information to enable the reconstruction of individual transactions.

(v) The Regulations also include requirements with respect to records to be kept when a service provider is relied on by another person and when the service provider is an introducer or an intermediary.

(vi) Records must be kept for 7 years from the date on which an occasional transaction is completed or the business relationship ends, or in the case transaction records, 7 years from when the transaction is completed and for all other records, 7 years from the date on which the business relationship end, unless the service provider's supervisory authority specifies a longer period.

Form of records

(vii) The Code requires records to be kept in a manner that will enable them to be readily retrieved. In practice this will require that records are kept:

(a) by way of original documents;

(b) by way of copies of original documents, certified where appropriate;

(c) as computerized or other electronic data;

(d) as scanned documents; or

(e) using a combination of the above.

Made this 3rd day of May 2017.

MAURICE EDWARDS
Director General of Finance and Planning
Chairman of the National Anti-Money
Laundering Committee.

Printed by the Government Printer at the Government Printing Office,
Campden Park, St. Vincent and the Grenadines.

2017 [Price $57.00]