Revised Regulations of Anguilla: P98-5

PROCEEDS OF CRIME ACT (R.S.A. c. P98)

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING CODE

Note: These Regulations are enabled under section 163 of the Proceeds of Crime Act, R.S.A. c. P98.

TABLE OF CONTENTS

PART 1

PRELIMINARY PROVISIONS

Interpretation

1. (1) In this Code—

"AML" means anti-money laundering;

"AML/CFT Regulations" means the Anti-Money Laundering and Terrorist Financing Regulations;

"Anguilla foundation" means a foundation established or continued in Anguilla under the Anguilla Foundations Act;

"board" means—

(a) in relation to a company, the board of directors, committee of management, Foundation Council 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 partnership, the partners, or in the case of a limited partnership, the general partners; or

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

"Code" means this Code;

"CFT" means combating terrorist financing;

"constitution", in relation to a legal entity, means the document or documents that constitute or define the constitution or formation of the legal entity and which set out the powers that regulate and bind the legal entity;

(R.A. 112/2022, s. 2)

"customer due diligence information" has the meaning specified in section 10(1)(a);

"director", in relation to a legal entity, means a person appointed to direct the affairs of the legal entity and includes—

(a) a person who is a member of the governing body of the legal entity; and

(b) a person who, in relation to the legal entity, occupies the position of director, by whatever name called;

"foundation" means a foundation, wherever established, and includes an Anguilla foundation;

"legal entity" includes a company, a partnership, whether limited or general, an association or any unincorporated body of persons, but does not include a trust;

"overseas foundation" means a foundation established in a jurisdiction other than Anguilla;

"POCA" means the Proceeds of Crime Act.

(2) Any word or phrase defined in POCA or the AML/CFT Regulations has, unless the context otherwise requires, the same meaning in this Code.

Scope of Code and Guidance

2. (1) This Code applies, to the extent specified, to—

(a) service providers within the meaning of the AML/CFT Regulations; and

(b) directors and boards of service providers.

(2) The Guidance provided under any section of this Code is not part of this Code but is Guidance issued under section 163(9) of POCA.

GUIDANCE

Introduction

(i) In common with all countries, both offshore and onshore, Anguilla 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 primarily set 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, Anguilla 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) Anguilla is committed to complying with its international obligations and has had a framework of anti-money laundering legislation in place since 1988 when the Drugs Trafficking Offences Act [then an Ordinance] was enacted. The legislative framework was extensively reviewed in 2008/2009 and a new Proceeds of Crime Act ("POCA") was enacted in July 2009. POCA consolidates the pre-existing provisions, which were previously to be found in a patchwork of different Acts, but also updates and reforms the law relating to money laundering. POCA is supported by the Anti-Money Laundering and Terrorist Financing Regulations ("the AML/CFT Regulations") and the Anti-Money Laundering and Terrorist Financing Code ("the Code").

In summary, POCA 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) provide the Unit, as Anguilla's Financial Intelligence Unit, with clear functions and enhance its powers;

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

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

(g) establish a National Forfeiture Fund; and

(h) by providing for the issuance of the AML/CFT Regulations and the Code, to enable the establishment of a framework for the prevention and detection of money laundering and terrorist financing.

(iii) POCA does not provide for the combating of terrorist financing, which is covered principally by the Anti-terrorism (Financial and Other Measures) Order 2002, which came into force on 1 August 2002. The Anti-terrorism Order is supplemented by the Al-Qaida (United Nations Measures) (Overseas Territories) Order 2012, the Afghanistan (United Nations Measures) (Overseas Territories) Order 2012 and the UK Terrorist Asset–Freezing Act.

(iv) Anguilla's service providers are one of the most important lines of defence against the use of the jurisdiction for money laundering and terrorist financing. The AML/CFT 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 AML/CFT Regulations constitute an offence for which the penalty is a maximum fine of $100,000. They also constitute a disciplinary violation, for which the maximum administrative penalty is $100,000. The AML/CFT Regulations are supplemented by the Code.

(v) The obligations contained in POCA, the AML/CFT Regulations and the Code will be rigorously enforced. However, it is in the interests of Anguilla 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 POCA, the AML/CFT 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 an Anguilla service provider in connection with money laundering or terrorist financing is likely to damage the reputation of the business and of Anguilla as a financial services jurisdiction, which could lead to a loss of legitimate business. It is therefore important that every service provider understands the important role it plays in protecting the reputation of Anguilla. Furthermore, a service provider that assists in the laundering of money or terrorist financing risks possible prosecution for a money laundering offence, enforcement action, administrative penalties and, if a regulated person, the loss of its licence. Breaches of POCA,

the AML/CFT Regulations and the Code could also result in the directors of a service provider being prosecuted for a criminal offence.

(vi) *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 Code sets out requirements imposed on service providers for the prevention of money laundering and the combating of terrorist financing that supplement the requirements of POCA and the AML/CFT Regulations. The Commission considers that the legal regime taken as a whole enables Anguilla to meet international standards.*

Purpose of the Code

(vii) *The purpose of the Code is to:*

(a) *set out detailed requirements for the prevention of money laundering and terrorist financing that must be met by service providers;*

(b) *assist service providers to design and implement appropriate systems and controls for the prevention of money laundering and terrorist financing;*

(c) *promote the use of a proportionate, risk-sensitive approach to the prevention of money laundering and terrorist financing and, in particular, to customer due diligence measures; and*

(d) *enable Anguilla to meet international standards concerning anti-money laundering and the combating of terrorist financing.*

(viii) *The Code and the Guidance cannot anticipate all circumstances and are not therefore exhaustive. Where permitted by the AML/CFT Regulations or the Code, service providers are expected to adopt an appropriate and intelligent risk-sensitive approach. The Code specifies minimum standards that must be complied with by every service provider, unless it is covered by a specific exemption. However, the particular circumstances of a service provider may require it to take additional measures beyond those minimum standards, and beyond the provisions of the Guidance. Service providers should always consider whether, on a case-by-case basis, additional measures are appropriate to prevent their products and services being used for money laundering or terrorist financing.*

It is therefore essential that all persons to whom this 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

(ix) *The Code has been issued by the Commission under section 163 of POCA, after consultation with Executive Council, and came into force on 31 July 2009. POCA*

provides that the Code is subordinate legislation and has full legislative effect. In the circumstances, the Code has the status of "law" in Anguilla.

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 POCA or the AML/CFT Regulations; and

(c) is enforceable by the Commission (see "Enforcement" below).

Breaches of the Code may constitute a disciplinary violation and, in certain circumstances, constitute an offence.

(x) POCA provides that the Code is subject to a negative resolution procedure. Although the Code has full effect on the date specified in the Code, it must be laid before the House of Assembly and the House may, by resolution, annul the Code at a subsequent meeting of the House.

Status of Guidance

(xi) The Guidance has been issued by the Commission under section 163(9) of POCA and, although provided with the Code, is not part of the Code. The purpose of the Guidance is to:

(a) outline the relevant requirements of POCA, the AML/CFT Regulations, the Code, the terrorist financing laws 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 POCA, the AML/CFT Regulations and the Code;

(c) provide important background or explanatory information;

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

(e) set out the factors that the Commission will take into account in considering whether or not a requirement in POCA, the AML/CFT Regulations or the Code has been complied with; and

(f) provide guidance on how the Commission expects service providers to comply with the AML/CFT Regulations and the Code.

(xii) Although the Guidance does not have the status of "law", section 162(5) of POCA requires the Court to consider whether a person has followed any guidance issued by the Commission in deciding whether a person has committed an offence under the AML/CFT Regulations. The Commission will also consider

whether the Guidance has been followed in deciding whether a service provider has failed to comply with the Code.

(xiii) In order to assist in explaining the AML/CFT framework, the Guidance paraphrases some of the requirements of POCA, the AML/CFT 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 cannot, of course, modify or in any way dilute the requirements of the AML/CFT Regulations or the Code. If there is any inconsistency between the Guidance and the AML/CFT Regulations or Code, the Regulations or the Code prevail.

(xiv) Although the Commission expects senior management of service providers to use the Code and the Guidance in the design of service providers' policies, systems and controls and in the preparation of service providers' procedures manuals, the Code and Guidance are not suitable for adopting by a service provider as its own procedures manual.

Scope of the Code

(xv) As indicated in section 2, 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 2 of the AML/CFT Regulations.

There are 3 types of service provider:

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

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

(c) 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.

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 entity, including partnerships, and individuals.

Application of Regulations and Code outside Anguilla

(xvi) Section 9 of the AML/CFT 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 in the foreign country permit. This is designed to ensure that Anguilla's relevant service providers apply standards

equivalent to the FATF Recommendations throughout their financial services business, wherever the business is situated or carried on.

(xvii) Where the laws of the foreign country do not permit this, the Commission must be informed in writing and, to the extent that the laws of the foreign country permit, the relevant 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

(xviii) The AML/CFT Regulations and the Code are enforceable:

(a) against regulated persons, by the Commission under the Financial Services Commission Act;

(b) against externally regulated service providers, by the Commission under Part 7 and Schedule 4 of POCA;

(c) against non-regulated service providers, by the Commission (as the designated supervisory body) under Part 7 and Schedule 4 of POCA.

(xix) Each of the above enables the Commission to take enforcement action if the service provider has contravened or is in contravention of the AML/CFT Regulations or the Code and provides the Commission with a range of enforcement powers, including the power to impose administrative penalties. In the case of a regulated person, non-compliance with the AML/CFT Regulations or the Code will also be taken into account by the Commission in assessing whether a regulated person is "fit and proper" to hold a licence.

(xx) Compliance by service providers with their AML/CFT obligations will form part of the Commission's assessment of service providers when undertaking on-site compliance visits. It will also form part of the Commission's on-going off-site monitoring of service providers.

Definitions of "company" and "legal entity"

(xxi) The term "company" is defined in POCA as "a body corporate, wherever incorporated, registered or formed" and includes a foundation. The term therefore covers all types of corporate body.

(xxii) The term "legal entity", however, includes partnerships, whether limited or general and any other type of association or unincorporated body of persons, except for trusts.

PART 2

POLICIES, PROCEDURES, SYSTEMS AND CONTROLS

Risk assessment

3. (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 and mitigate those risks; and
R.A. 112/2022, s. 3(a)(i)

(c) designing, establishing, maintaining and implementing AML/CFT policies, procedures, systems and controls that comply with the requirements of the AML/CFT Regulations and this Code and that are appropriate for the risks that it faces.
R.A. 112/2022, s. 3(a)(ii)

(2) The risk assessment carried out by a service provider under subsection (1) shall—

(a) take into account any relevant warnings, information, advice or guidance issued by the Unit or the Commission relevant to the service provider's risk assessment;

(b) consider all relevant risk factors, taking particular account of risk factors relating to—

(i) its customers,

(ii) the countries or geographic areas in which it operates,

(iii) its products and services,

(iv) its transactions, and

(v) its delivery channels; and

(c) take into account—

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

(ii) the size, nature and complexity of its business.
(R.A. 112/2022, s. 3(b))

(3) A service provider must, on the request of the supervisory authority, provide the supervisory authority with the risk assessment that it has prepared under subsection (1) and the information on which that risk assessment was based.
(R.A. 112/2022, s. 3(b))

(4) A service provider shall regularly review and update the risk assessment if there are material changes to any of the matters specified in subsection (2).
(R.A. 112/2022, s. 3(c))

Responsibilities of board

4. (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 subsection (1), the board of a service provider has the following responsibilities—

(a) undertaking the risk assessment required by section 3;

(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, systems and controls established and promptly taking such actions as is required to remedy deficiencies.

Policies, procedures, systems and controls

5. (1) Without limiting section 17 of the AML/CFT Regulations, the policies, procedures, systems and controls established, maintained and implemented by a service provider under that section 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 Anguilla.

(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 shall—

(a) ensure that the policies, procedures, systems and controls established under section 17 of the AML/CFT Regulations are regularly reviewed and updated; and

(b) maintain a written record of—

(i) any changes to the policies, procedures, systems and controls made as a result of the review and update required by paragraph (a), and

(ii) the steps taken to communicate those policies, procedures, systems and controls, or any changes to them, to relevant persons within the service provider's business.

(4) The policies, procedures, systems and controls must be—

(a) proportionate with regard to the size and nature of the service provider's business; and

(b) approved by its board or senior management.

(5) The policies, procedures, systems and controls must include reliance on introducers and intermediaries.

(6) 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 AML/CFT Regulations and this Code.

(R.A. 112/2022, s. 4)

Outsourcing

6. (1) Subject to subsection (2), a service provider may outsource AML/CFT activities, including obligations imposed by the AML/CFT 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 Commission 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, 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 MLRO.

(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 Commission 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.

GUIDANCE

Risk-sensitive approach

(i) The senior management of companies and other undertakings, both within and outside the financial sector, increasingly manage the affairs of their undertaking

with regard to the risks inherent in its business and put in place systems, controls and procedures 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 provider in Anguilla, 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."

Anguilla's 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. Section 3(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 section 3(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) Section 3(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 Commission 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, however. 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 sections of the Code.

Responsibilities of board

(xi) The principal responsibilities of the board are set out in section 4 of the Code. The Board will be assisted in fulfilling these responsibilities by the MLRO, the MLCO 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, procedures, systems and controls

(xii) Section 17 of the AML/CFT 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) 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;

(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 section 5 of the Code.

To be effective, the AML/CFT systems and controls must be appropriate given the circumstances of a particular service provider.

(xiii) Section 4(2)(d) of the Code provides that the board has responsibility for assessing the effectiveness of, and compliance with, the policies, 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 MLCO and the MLRO;

(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 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 MLCO.

(xvi) Section 5(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) Section 5(6) 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, it must appoint one or more employees to be responsible for testing compliance with its AML/CFT policies, procedures, systems and controls. The employee or employees concerned must be independent. For example, the audit function cannot be

performed by any employee having responsibility for the compliance function or any employee who is, or has been, involved in the design of the policies, procedures, systems and controls. Alternatively, 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) Section 6(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.

Money laundering reporting officer

7. (1) Subject to subsection (2), the MLRO appointed by a service provider pursuant to section 23 of the AML/CFT Regulations shall—

(a) be an employee of the service provider or of a company in the same group as the service provider and shall be based in Anguilla;

(b) have the appropriate skills and experience and otherwise be fit and proper to act as the service provider's MLRO;

(c) possess sufficient independence to perform his role objectively;

(d) have sufficient seniority in the organisational structure of the licensee to undertake his responsibilities effectively and, in particular, to enable the MLRO to have direct access to the board with respect to AML/CFT matters; and

(e) have sufficient resources, including time, to perform the function of MLRO effectively.

(2) A service provider may apply to the Commission for an exemption from paragraph (1)(a).

Money laundering compliance officer

8. (1) Subject to subsection (2), the MLCO appointed by a service provider pursuant to section 22 of the AML/CFT Regulations shall—

(a) be an employee of the service provider or of a company in the same group as the service provider and shall be based in Anguilla;

(b) have the appropriate skills and experience and otherwise be fit and proper to act as the service provider's MLCO;

(c) possess sufficient independence to perform his role objectively;

(d) have sufficient seniority in the organisational structure of the licensee to undertake his responsibilities effectively and, in particular, to ensure that his requests, where appropriate, are acted upon by the service provider and its staff and his recommendations properly considered by the board;

(e) report regularly, and directly, to the board and have regular contact with the board;

(f) have sufficient resources, including time, to perform the functions of MLCO effectively; and

(g) have unfettered access to all business lines, support departments and information necessary to perform the functions of MLCO effectively.

(2) A service provider may apply to the Commission for an exemption from paragraph (1)(a).

GUIDANCE

Money laundering reporting officer

(i) Section 23 of the AML/CFT Regulations requires every service provider to appoint a MLRO. The MLRO has responsibility for receiving internal money laundering disclosures, deciding whether these disclosures should be reported to the Unit and, if he so decides, making the reports to the Unit, and acting as the liaison point with the Unit and the Commission.

(ii) A service provider with a substantial business may need to appoint other individuals to assist the MLRO. 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 MLRO. However, the MLRO has ultimate responsibility for all reports made by employees of the service provider and any other individuals appointed must be answerable to the MLRO.

(iii) The MLRO will have more knowledge and experience relevant to the prevention of money laundering and terrorist financing than other employees of the service provider. The AML/CFT Regulations anticipate that the MLRO 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 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 MLRO is expected to act as a filter and not to routinely pass all disclosures made to him to the Unit without making his own assessment.

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

(v) The MLRO must:

(a) oversee any deputy MLRO 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 MLRO must also take great care to manage relationships with clients appropriately to avoid tipping off any third parties.

Money laundering compliance officer

(vii) Section 22 of the AML/CFT Regulations requires every service provider to appoint a MLCO. The MLCO can be the same person as the MLRO 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 Commission.

However, a regulated person may split the reporting and compliance functions and appoint different individuals as its MLRO and MLCO.

PART 3

CUSTOMER DUE DILIGENCE

Scope and interpretation

9. (1) This Part applies to customer due diligence measures that a service provider is required to apply by the AML/CFT Regulations.

(2) For the purposes of this Part, a branch or subsidiary is a "qualifying branch or subsidiary" if it is part of—

(a) a group of companies that has its head office in a country—

(i) that is subject to legal requirements in its home country for the prevention of money laundering and terrorist financing that are consistent with the requirements of the FATF Recommendations, and

(ii) is subject to effective supervision for compliance with those legal requirements by a foreign regulatory authority; or

(b) a group headquartered in a well-regulated country which applies group standards to subsidiaries and branches worldwide, and tests the application of, and compliance with, such standards.

Customer due diligence measures to be applied by service provider

10. (1) A service provider shall—

(a) obtain customer due diligence information on every customer, third party and beneficial owner comprising—

(i) identification information in accordance with section 15, 17, 20 or 22 of this Code as the case may be, and

(ii) relationship information in accordance with section 11 of this Code;

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

(c) on the basis of the information obtained under paragraphs (a) and (b), prepare and record a risk assessment with respect to the customer;

(d) 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 in accordance with section 3(1)(e) of the AML/CFT Regulations and the relevant sections of this Code; and

(e) periodically update the customer due diligence information that it holds and adjust the risk assessment that it has made accordingly.

(R.A. 112/2022, s. 5)

(2) In preparing a risk assessment with respect to a customer, a service provider shall take account of all relevant risks and shall consider, in particular, the relevance of the following risks—

(a) customer risk;

(b) product risk;

(c) delivery risk; and

(d) country risk.

(3) Where a service provider is required by the AML/CFT Regulations or this Code to verify the identity of a person, it shall verify that person's identity using documents, data or information obtained from a reliable and independent source.

(4) This section does not limit the requirements of the AML/CFT Regulations.

(5) For the purposes of this section, "beneficial owner", with respect to a customer, means a beneficial owner of the customer or of a third party.

Relationship information

11. (1) For the purposes of this Code, relationship information is information concerning the business relationship, or proposed business relationship, between the service provider and the customer.

(2) 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 Anguilla, the reason for using a service provider based in Anguilla; and

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

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

(a) the type of trust or legal entity;

(b) the nature of the activities of the trust or legal entity 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 entities, and

(ii) classes of beneficiaries or charitable objects;

(d) in the case of a legal entity, its ownership and, where the legal entity 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 entity is subject to supervision in or outside Anguilla and, if so, details of the relevant supervisory body.

GUIDANCE

Introduction

(i) The maintenance and operation by the financial services sector of adequate customer due diligence measures is, and has for many years, been fundamental to Anguilla's efforts to combat money laundering and terrorist financing.

(ii) A service provider needs to 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 MLRO and employees, to assess whether a suspicion activity report should be made.

What is "customer due diligence"?

(iv) The term "customer due diligence measures" is defined in section 3 of the AML/CFT Regulations. In essence, effective customer due diligence measures will require a service provider to carry out a number of steps, addressing:

(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 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 AML/CFT 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.

Summary of principal requirements of AML/CFT Regulations with respect to customer due diligence

(vi) Section 10(1) of the AML/CFT 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 a one-off 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) Section 17(1) of the AML/CFT 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) Section 17(2) of the AML/CFT 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; or

(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) Section 12 of the AML/CFT 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 AML/CFT 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

to Part 2 of the Code and this Guidance should be read together with the Guidance in Part 2. However, it should, of course, be appreciated that the minimum requirements of the AML/CFT Regulations and the Code must at all times be complied with.

(xi) Section 3 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 this Part.

(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 following the steps set out in section 3(2) of the Code.

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 sections of the Code. The Guidance 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 principal 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, section 11(2) of the Code sets out relationship information that must always be obtained by a service provider.

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. It should be noted that it is the source of the person's wealth that is important rather than the amount of it. It may not, therefore, be necessary for information on the amount of wealth to be obtained.

(xviii) Section 11(2)(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.

(xix) When sufficient customer due diligence information has been obtained, the service provider should carry out a customer risk assessment. Section 10(2) of the Code 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 Anguilla legislation applying United Nations sanctions, guidance issued by the Commission 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. In particular, the UK Government Treasury maintains a consolidated list of targets listed by the United Nations, European Union and UK under legislation relating to current financial sanctions regimes.*

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; and

(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) Section 10(1)(b) of the AML/CFT Regulations requires a service provider to apply customer due diligence measures subsequent to the establishment of a business relationship (i.e. 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; and

(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 Commission 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 5 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.

Enhanced due diligence

12. Without limiting section 12 of the AML/CFT Regulations, a service provider shall apply enhanced due diligence measures and undertake enhanced ongoing monitoring where a customer, transaction or business relationship involves—

(a) private banking, legal entities or arrangements, including trusts, that are personal asset holding vehicles; or

(b) companies that have nominee shareholders or shares in bearer form.

Foreign politically exposed persons

13. (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 a 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) Subsection (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 person 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) Subsections (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

14. (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 paragraph (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 subsection (1)(a), (b) or (c), section 12 applies as if the person were a foreign politically exposed person.

GUIDANCE

Enhanced customer due diligence - introduction

(i) Section 12(2) of the AML/CFT 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 domestic bank that has or proposes to have a banking or similar relationship with an institution whose address for that purpose is outside Anguilla;

(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 third party;

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

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

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

(ii) Section 12 of the AML/CFT Regulations sets out a number of specific circumstances where enhanced customer due diligence measures must be applied and enhanced ongoing monitoring undertaken. However, 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 guidance below with respect to politically exposed persons).

Enhanced customer due diligence measures and ongoing monitoring

(iii) Section 12(1) of the AML/CFT 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 AML/CFT 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 Anguilla or in a country other than Anguilla, or who are, or have been, entrusted with a prominent function by an international organisation. Immediate family members and close associates of PEPs are to be treated as if they were PEPs.

(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 AML/CFT Regulations provide a comprehensive definition of a PEP (section 5). 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. Section 5 includes 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) Section 12 of the AML/CFT 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 section 13 of the Code supplements 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 section 3 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 AML/CFT 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) Assessing 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) Ascertaining 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, determining whether the person concerned has any associations with those individuals. The websites of international organisations, such as the United Nations, may assist in determining the identity of such individuals.

(xii) The above checks do not represent a comprehensive list and the Commission would expect them to be used on a risk-sensitive basis. The extent to which a service provider needs to utilise 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

15. (1) A service provider shall obtain the following identification information with respect to an individual who it is required by the AML/CFT 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

16. (1) A service provider shall—

(a) verify the identity of an individual where required by the AML/CFT 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 paragraph (1)(b), the following represent changes of an individual's identity within the meaning of that paragraph—

(a) marriage;

(b) change of nationality; and

(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 2 independent sources, 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.

GUIDANCE

Introduction

(i) Sections 15 to 28 of the Code provide for, and the following Guidance describes:

(a) the identification information that must be obtained by a service provider in applying customer due diligence measures (and ongoing monitoring, which is covered in a separate Part of the Code);

(b) the verification of the identity information; and

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

This Guidance also covers the requirements of the AML/CFT Regulations concerning the obtaining and verification of identity evidence.

Requirements of AML/CFT Regulations

(ii) As indicated in the Guidance to previous sections of the Code, the AML/CFT Regulations [section 3(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 meaning of "beneficial owner" is contained in section 1 of the AML/CFT 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.

It should be noted that it makes no difference whether:

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

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

(iv) As indicated in the guidance to the sections on customer due diligence above, section 10 of the AML/CFT Regulations specifies when customer due diligence measures must be applied. These circumstances are supplemented by section 10 of the Code.

(v) 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, section 10(5) and (6) of the AML/CFT Regulations permit two exceptions. Subsection (5) 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.

(vi) Section 10(6) of the AML/CFT 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.

(vii) 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

(viii) 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.

(ix) 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 Anguilla, 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

(x) A service provider is required by the AML/CFT 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.

(xi) Section 15(1) of the Code sets out the identification that must always be obtained with respect to an individual. Section 15(2) requires a service provider to obtain additional identity information where it determines that the individual presents a higher risk and section 15(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

(xii) It is an overriding requirement of both the AML/CFT 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.

(xiii) Evidence of identity can take a number of forms. In respect of individuals, much weight is placed on identity documents, such as passports, and 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. If a service provider is not familiar with the form of evidence obtained to verify identity, it may be necessary for the service provider to take appropriate measures to satisfy itself that the evidence is genuine.

(xiv) 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 set out in the following paragraphs. Service providers are reminded that section 162(5) of POCA provides that, in deciding whether a person has committed an offence under the AML/CFT Regulations, the Court shall consider whether the person has followed any guidance issued by the Commission.

(xv) The Commission regards the following general methods of verifying the identity of an individual to be acceptable:

(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; and

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

(xvi) The Commission 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 may be verified using:

(a) an Anguilla full (ie not a temporary) driver's licence; 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

(xviii) 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.

(xix) In principle, the Commission 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 Commission 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.

(xx) 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 entities (other than foundations)

17. (1) This section and sections 18 and 19 apply to a legal entity other than a foundation.

(2) A service provider shall obtain the following identification information with respect to a legal entity that it is required by the AML/CFT Regulations or this Code to identify—

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

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

(c) the legal form of the legal entity, the law under which it is governed and the powers that regulate and bind it;

(R.A. 112/2022, s. 6(a)(i))

(d) any official identifying number;

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

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

(g) the mailing address of the legal entity;

(h) the principal place of business of the legal entity;

(i) the names of the directors of the legal entity and of the senior persons responsible for the management and operation of the legal entity;

(R.A. 112/2022, s. 6(a)(ii))

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

(k) identification information on individuals who are beneficial owners.

(R.A. 112/2022, s. 6(a)(iii))

(3) A service provider must obtain sufficient information under this section to enable it to understand the ownership and control structure of the legal entity.

(R.A. 112/2022, s. 6(b))

(4) Where a service provider determines that a legal entity 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 entity as it considers appropriate.

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

(6) Where identification information on an individual, as a director or beneficial owner, is required to be obtained, section 15 applies.

Verification of identity, legal entities (other than foundations)

18. (1) A service provider shall—

(a) verify the identity of a legal entity where required by the AML/CFT Regulations to do so; and

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

(2) A service provider shall, using evidence from at least one independent source, verify—

(a) the name of the legal entity;

(b) the company number, registration number or other official identifying number of the legal entity;

(c) the date and country of its incorporation, registration or formation and the law under which the legal entity is governed;

(d) the constitution of the legal entity;

(e) the address of the legal entity's registered office or, if it does not have a registered office its head office and, if different, its principal place of business;

(f) to the extent not verified under paragraphs (a) to (d), proof of the legal entity's existence; and

(g) to the extent not verified under paragraph (d), evidence of the powers that regulate and bind the legal entity.

(R.A. 112/2022, s. 7)

(3) Where a service provider determines that a legal entity, 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 entity's identification as it considers appropriate.

(4) A document used to identify the identity of a legal entity 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

19. (1) Where required by the AML/CFT Regulations to verify the identity of a legal entity, a service provider must—

(a) verify the names of the directors of the legal entity;

(b) verify the names of the senior persons responsible for the management and operation of the legal entity; and

(c) if section 3(2) and (3) of the AML/CFT Regulations apply, take reasonable measures to verify the identity of the individual who holds the position of senior managing official in the legal entity.

(R.A. 112/2022, s. 8(a))

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

(3) Where subsection (2) applies, but without limiting it, a service provider shall verify the identity of each director of the legal entity.

(R.A. 112/2022, s. 8(b))

(4) Where the identity of an individual, as director or beneficial owner, is required to be verified, section 15 applies.

GUIDANCE

Introduction

(i) Sections 17 to 19 of the Code specify requirements concerning the identification of, and the verification of the identity of, legal entities, other than foundations. Foundations are covered in sections 22 and 23 of the Code. A legal entity is defined in the AML/CFT 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 entity

(ii) There is a wide range of potential customers that are not individuals. These include legal entities (such as companies) and trusts (which are not legal entities and are covered separately in sections 20 and 21 of the Code). The legal owners of a legal entity may be specific individuals or other legal entities. 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 entity 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 entity 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 entity 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 entity and, potentially, some of the individuals behind it should be obtained.

(v) Whilst information on a legal entity'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 entity, a service provider should ensure that it fully understands the legal form, structure and ownership of the legal entity and should obtain sufficient additional information on the nature of the entity's business, and the reasons for seeking the product or service.

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

(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) Section 18(1) of the Code sets out the identification that must always be obtained with respect to a legal entity. Section 18(3) requires a service provider to obtain additional identity information where it determines that the legal entity presents a higher risk.

Verification of identity of a legal entity

(ix) The Commission regards the following general methods of verifying the identity of a legal entity to be acceptable:

(a) certificate of incorporation, registration or equivalent;

(b) memorandum and articles of association or equivalent constituting documents;

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

(d) the latest audited financial statements of the legal entity;

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

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

(x) Where the service provider determines that the legal entity presents a low level of risk, at least one of the methods specified above should be used. Where it determines that the legal entity presents a higher level of risk, at least 2 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, section 25 of the Code applies.

(xiii) In the case of a legal entity 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

20. (1) Where a service provider is required by the AML/CFT Regulations or this Code to identify a trust, it shall—

(a) obtain the following—

(i) the name of the trust,

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

(iii) any official identifying number,

(iv) the legal form of the trust, including the type of trust,

(v) the law under which the trust is governed and the powers that regulate and bind it,

(vi) identification information on each beneficial owner of the trust,

(vii) the names of any persons, other than the trustees, that have a senior management position in relation to the trust or the trust property, and

(viii) the mailing address of the trustees; and

(R.A. 112/2022, s. 9(b))

(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) A service provider must obtain sufficient information under this section to enable it to understand the nature of trust's business and the ownership and control structure of the trust.

(R.A. 112/2022, s. 9(c))

(3) Where a service provider determines that a trust 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 trust as it considers appropriate.

(R.A. 112/2022, s. 9(c))

(4) Identification information required to be obtained on any person under this section shall be obtained in accordance with section 15 if the person is an individual, section 17 if the person is a legal entity or section 22 if the person is a foundation.

Verification of identity, trusts and beneficial owners

21. (1) Where a service provider is required by the AML/CFT Regulations to verify the identity of a trust, it shall—

(a) verify—

(i) the name and date of establishment of the trust,

(ii) the legal form of the trust and the law under which the trust is governed,

(iii) the trust deed and any other document that regulates and binds the operation of the trust,

(iv) the appointment of each trustee and the nature of the trustees' duties,

(v) the names of any persons, other than the trustees, that have a senior management position in relation to the trust or the trust property,

(vi) the mailing address for the trustees,

(vii) to the extent not verified under subparagraphs (i) to (vi), proof of the trust's existence, and

(viii) to the extent not verified under subparagraph (iii), evidence of the powers that regulate and bind the legal entity; and

(b) take reasonable measures to verify the identity of each beneficial owner of the trust.
(R.A. 112/2022, s. 10(b))

(2) Where a service provider determines that a trust that it is required to identify presents a higher level of risk, the service provider shall verify such other components of the trust's identity as it considers appropriate.
(R.A. 112/2022, s. 10(b))

(3) A document used to verify the identity of a trust or a person specified in this section 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 section to be verified shall—

(a) if the person is an individual, be verified in accordance with section 16;

(b) if the person is a legal entity, be verified in accordance with section 18; or

(c) if the person is a foundation, be verified in accordance with section 23.

GUIDANCE

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 AML/CFT 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 sections of the Code relating to individuals, legal entities 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 entity or a foundation.

Identification information, foundations and similar legal arrangements

22. (1) A service provider shall obtain the following identification information with respect to a foundation that it is required by the AML/CFT 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) the type of foundation;
(R.A. 112/2022, s. 11(b)(i))

(d) the law under which the foundation is governed and the powers that regulate and bind it;
(R.A. 112/2022, s. 11(b)(i))

(e) any official identifying number;

(f) the registered address of an Anguilla foundation (or the equivalent for an overseas foundation) or, if an overseas foundation does not have a registered address (or equivalent), the address of the head office of the foundation;

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

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

(i) the name and address of the registered agent of an Anguilla foundation (or the equivalent for an overseas foundation, if any);

(j) the name and address of the Secretary of an Anguilla foundation, if any (or the equivalent for an overseas foundation, if any);

(k) identification information on each beneficial owner of the foundation; and
(R.A. 112/2022, s. 11(b)(ii))

(l) the names of any persons, other than the Foundation Council members, that have a senior management position in relation to the foundation or its operation or whose approval is required for any decision.
(R.A. 112/2022, s. 11(b)(ii))

(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 considers appropriate.

(3) Identification information required to be obtained on any person under this section shall be obtained in accordance with section 15 if the person is an individual or section 17 if the person is a legal entity.

(4) Notwithstanding subsection (1), the service provider may require any other identification information that the service provider deems necessary to aid in identifying the foundation.

(5) A service provider must obtain sufficient information under this section to enable it to understand the nature of the foundation's business and the ownership and control structure of the foundation.

(6) A service provider shall apply this section to the identification of a legal arrangement that is similar to a foundation, with such modifications as are necessary and appropriate.
(R.A. 112/2022, s. 11(d))

Verification of identity, foundations and similar legal arrangements

23. (1) A service provider shall, using evidence from at least one independent source, verify—

(a) the name and date of establishment, registration, formation or incorporation of the foundation;

(b) the legal form of the foundation and the law under which the foundation is governed;

(c) the constitution of the foundation and any other document that regulates and binds the operation of the foundation;

(d) the names of the Foundation Council members;

(e) the names of any persons, other than the Foundation Council members that have a senior management position in relation to the foundation or its operation or whose approval is required for any decision;

(f) the registered address, or equivalent, or if the foundation does not have a registered address, the address of the head office and, if different, its principal place of business;

(g) to the extent not verified under paragraphs (a) to (c), proof of the foundation's existence; and

(h) to the extent not verified under paragraph (c), evidence of the powers that regulate and bind the legal entity.

(R.A. 112/2022, s. 12(b))

(2) A service provider shall take reasonable measures to verify the identity of each beneficial owner of the foundation.

(R.A. 112/2022, s. 12(b))

(3) 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.

(4) 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.

(5) A person whose identity is required by this section to be verified shall—

(a) if the person is an individual, be verified in accordance with section 16; or

(b) if the person is a legal entity, be verified in accordance with section 18.

(R.A. 112/2022, s. 12(c))

(6) A service provider shall apply this section to the verification of identification of a legal arrangement that is similar to a foundation, with such modifications as are necessary and appropriate.

(R.A. 112/2022, s. 12(d))

Identification and verification of any other legal arrangement

24. (1) Where a service provider is required by the AML/CFT Regulations or this Code to identify and verify a legal arrangement other than a trust or a foundation (or a legal arrangement similar to a foundation), the service provider shall—

(a) determine the beneficial owners of the legal arrangement in accordance with section 12 of the Commercial Registry and Beneficial Ownership Registration System Act; and

(b) apply sections 18 to 21 of that Act, with such modifications as are appropriate.

(2) In applying the definition of "beneficial owner" in the Commercial Registry and Beneficial Ownership System Registration Act to this Code, "settlor" includes a person who, as a settlor, established the trust and any person who has, at any time, subsequently settled assets into the trust.

(R.A. 112/2022, s. 14)

GUIDANCE

(i) Sections 22 and 23 of the Code specify requirements concerning the identification of, and the verification of the identity of, foundations.

(ii) Where a service provider is required to identify a foundation, certain identification information (as specified in the Code) should be obtained as a standard requirement. Thereafter, on the basis of the money laundering/terrorist financing risk assessed in the customer risk assessment, a service provider should decide the extent to which the identity of the foundation 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 foundation and, potentially, some of the individuals concerned with it should be obtained.

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

(iv) A service provider is required by the AML/CFT 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) Section 22(1) of the Code sets out the identification that must always be obtained with respect to a foundation. Section 22(2) requires a service provider to obtain additional identity information where it determines that the foundation presents a higher risk.

(vi) The Commission 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, section 25 of the Code applies.

(ix) In the case of a foundation that is a regulated person, the identity of a Foundation Council member may be verified if the full name of the member is obtained together with written confirmation from the regulated person that the person concerned is a Foundation Council member.

Non face-to-face business

25. 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 AML/CFT 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

26. (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.

GUIDANCE

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.

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.

(iii) 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 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.

(iv) 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.

(v) 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 check 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

(vi) 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.

(vii) 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, or a serving police or customs officer;

(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.

(viii) The Code requires that the certifier must have provided adequate information so that he may be contacted in the event of a query. The Commission considers that this requirement would be met when the certifier includes 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

27. 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 section 15 of the AML/CFT Regulations, the service provider shall obtain and retain documentation establishing that section 15 applies.

GUIDANCE

(i) Section 15 of the AML/CFT Regulations specifies circumstances in which a service provider is not required to apply customer due diligence measures before establishing a business relationship or 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 recognised exchange, or a public authority in Anguilla; 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 AML/CFT Regulations define a recognised exchange as an exchange that is a member of the World Federation of Exchanges. However, section 1(4) of the AML/CFT Regulations provides that an exchange is not a recognised exchange if it is situated in a country specified by the Commission as a country that does not implement, or does not effectively apply, the FATF Recommendations or the Commission 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 Anguilla:

(a) the Government of Anguilla;

(b) any statutory body established under an Anguilla enactment; and

(c) any company wholly owned by the Government of Anguilla.

Intermediaries and introducers

28. (1) Before relying on an intermediary or an introducer to apply customer due diligence measures in accordance with section 14 of the AML/CFT 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 that is—

(i) subject to requirements in relation to customer due diligence and record keeping which are equivalent to those set out in the FATF Recommendations, and

(ii) effectively supervised for compliance with those requirements;

(R.A. 112/2022, s. 15)

(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 paragraph (1)(b) and any additional risk mitigation measures it considers appropriate; and

(b) retain in its records—

(i) the assurances obtained under section 14(2) of the AML/CFT Regulations and the confirmations that it has obtained under paragraph (1)(c), and

(ii) the information that it has sought and obtained under paragraph (1)(d).

GUIDANCE

Introduction

(i) The AML/CFT 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) 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 where, following the introduction, a direct relationship between the service provider and the underlying customer. The terms "intermediary" and "introducer" are defined in section 1(1) of the AML/CFT 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 section 14 of the AML/CFT 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; and
(b) the intermediary or introducer consents to being relied on.

(vii) The AML/CFT 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 AML/CFT 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.

(ix) 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.

(x) Section 14(3) of the AML/CFT 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 Commission, on its request, without delay. The phrase "without delay" means as close to immediately as possible. The AML/CFT 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 Commission would not accept a delay of more than 72 hours as being reasonable.

PART 4

MONITORING CUSTOMER ACTIVITY

Ongoing monitoring policies, procedures, systems and controls

29. (1) The ongoing monitoring policies, procedures, systems and controls established by a service provider in accordance with section 17 of the AML/CFT Regulations shall—

(a) provide for a more thorough scrutiny of higher risk customers including politically exposed persons and close family and associates of politically exposed persons;
(R.A. 112/2022, s. 16(a))

(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 with countries against which the FATF calls for countermeasures, or

(ii) which are the subject of United Nations or European Union countermeasures; and
(R.A. 112/2022, s. 16(b))

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

GUIDANCE

Requirements of the AML/CFT Regulations concerning ongoing monitoring

(i) Section 10(3) of the AML/CFT Regulations require a service provider to undertake ongoing monitoring of a business relationship. Ongoing monitoring is defined in section 4 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) Section 29(1) of the Code requires a service provider to have policies, procedures, 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) Section 12(2) of the AML/CFT 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 domestic bank that has or proposes to have a banking or similar relationship with an institution whose address for that purpose is outside Anguilla;

(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 procedures, systems and controls are that:

(a) they flag up 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 unauthorised 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 of 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 5

REPORTING SUSPICIOUS ACTIVITY AND TRANSACTIONS

Reporting procedures

30. (1) A service provider shall establish and maintain reporting procedures that—

(a) communicate the identity of the MLRO to its employees;

(b) require that a report is made to the MLRO 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 MLRO 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 MLRO 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, and in any event within 24 hours, by the MLRO to the Unit in writing, where the MLRO knows, suspects or has reasonable grounds to know or suspect that another person is engaged in money laundering or terrorist financing; and

(R.A. 112/2022, s. 17 and s. 25)

(f) require the MLRO to report to the Unit 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.

(R.A. 112/2022, s. 25)

(2) For the purposes of this section, MLRO includes any deputy MLRO that may be appointed.

Internal reporting procedures

31. (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 MLRO 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 MLRO;

(f) suspicious activity reports to be acknowledged by the MLRO.

(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 by MLRO

32. A service provider shall ensure that—

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

(b) each suspicious activity report is considered by the MLRO in light of all relevant information; and

(c) the MLRO documents the evaluation process followed and reasons for the decision to make a report or not to make a report to the Unit.

(R.A. 112/2022, s. 25)

Reports to Unit

33. (1) A service provider shall require the MLRO to make external suspicious activity reports directly to the Unit as soon as practical that—

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

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

(2) The information required to be included in a report to the Unit for the purposes of subsection (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 Unit may require.

(R.A. 112/2022, s. 25)

GUIDANCE

Introduction

(i) POCA and the terrorist financing laws contain disclosure requirements concerning knowledge or suspicion (or grounds for knowledge or suspicion) of money laundering or terrorist financing. Part 5 of the Code and the Guidance that follows are designed to outline and amplify the statutory disclosure requirements. The obligations to disclose are so important that they are set out in detail in this Guidance.

Statutory requirements POCA

(ii) Section 122 of POCA requires a person to make a disclosure to the Unit or his MLRO if the person:

(a) knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering; and

(b) the information or other matter on which his 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.

(iii) It is beyond the scope of this Guidance to consider the money laundering offences themselves, but broadly, there are three:

(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 offences.

(iv) 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.

(v) All service providers are required by the AML/CFT Regulations to establish procedures for the reporting of disclosures. This applies both to internal reports, i.e. disclosure reports within the service provider to the MLRO and external reports, i.e. disclosure reports to the 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 Unit. Provided an employee does this, the employee will not commit an offence under section 122 of POCA. Although the term "suspicious activity report" is used, the disclosure in the report could be one of knowledge, rather than suspicion.

(vi) The effect of section 118 of POCA 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 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.

(vii) A person who fails to make a report when required to do so, in accordance with section 122, commits an offence. As indicated above, an offence may be committed not just by the service provider but also by its employees.

Statutory requirements (terrorist financing disclosures)

(viii) There are 4 Orders that contain mandatory reporting requirements with respect terrorist financing. These are:

(a) the Anti-terrorism (Financial and Other Measures) (Overseas Territories) Order 2002;

(b) the Terrorist Asset–Freezing etc. Act 2010 of the United Kingdom as extended to Anguilla by the Terrorist Asset-Freezing etc. Act 2010 (Overseas Territories) Order 2011;

(c) the Al-Qaida (United Nations Measures) (Overseas Territories) Order 2012; and

(d) the Afghanistan (United Nations Measures) (Overseas Territories) Order 2012.

(ix) With respect to service providers and terrorist financing disclosures, the obligations in the above Orders are similar in effect to the money laundering disclosure obligations in POCA outlined above. A wider consideration of the Orders is beyond the scope of this Guidance. One of the Orders provides that a terrorist financing disclosure may be made to a "constable" and others require terrorist financing disclosures to be made to the Governor. POCA enables the Unit to receive such disclosures that would otherwise be made to a constable and the relevant Orders allow the Governor to delegate responsibility in relation to disclosures, which has been done. Accordingly, service providers should ensure that terrorist financing disclosures are always made to the Unit rather than directly to a police officer or to the Governor.

Offences involving or relating to tax

(x) Criminal conduct is defined in POCA as "conduct which constitutes an offence or would constitute an offence if it had occurred in Anguilla". 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 one year or more.

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

(xii) 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, that is, the offence that results in proceeds of crime, may be a tax offence or may involve or relate to tax, and their reporting procedures should reflect this.

PART 6

EMPLOYEE TRAINING AND AWARENESS

Training and vetting obligations

34. (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 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) explain the meaning of "money laundering" for the purposes of POCA, the AML/CFT Regulations and this Code, cover the legal obligations of employees to make disclosures under section 122 of POCA and explain the circumstances in which such disclosures are required to be made;

(c) explain the risk-based approach to the prevention and detection of money laundering and terrorist financing;

(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.

GUIDANCE

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 recognise 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) It is for these reasons that the AML/CFT Regulations and the Code contain a number of requirements concerning staff training and awareness.

Statutory requirements

(v) Section 21 of the AML/CFT Regulations contains the following requirements with respect to training and employee awareness:

A service provider must 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 or an applicable Code;

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

(c) the Regulations, applicable Codes and any Guidance issued by the Commission or a supervisory authority.

(vi) A service provider must provide employees specified in section 21(1) of the AML/CFT Regulations 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 techniques, methods, trends and typologies.

(viii) The requirements of the AML/CFT 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 are 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 requesting and verifying details of any criminal convictions.

Staff awareness

(xiii) The requirements of the AML/CFT 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 POCA, terrorist financing laws, the AML/CFT Regulations, any applicable Code and any Guidance issued by the Commission 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 AML/CFT Regulations, a service provider will have 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 122 of POCA;

(c) the potential implications to the service provider for any breaches of POCA, the AML/CFT 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 POCA, the terrorist financing laws, the AML/CFT Regulations and any applicable Code;

(c) requiring employees to acknowledge that they have received and understood the business' procedures manual and 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 POCA, the terrorist financing laws, the AML/CFT Regulations and any applicable Code. Given the risk-sensitive approach adopted by the Anguilla regime, every service provider will have to put in place its own systems and controls and procedures that are appropriate for its business.

(xvii) Section 34(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 MLRO 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 POCA, the

terrorist financing laws and the AML/CFT Regulations and providing some basic information concerning this Code; and

(c) require employees to acknowledge that they have received and understood the business' 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 Anguilla and internationally.

Staff training

(xix) The AML/CFT 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. 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;

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

(c) 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.

(xx) Section 34(2)(b) of the Code provides that the training should explain the meaning of the term "money laundering". 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 122 of POCA 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.

(xxi) Section 34(1)(a) 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 Commission 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 procedures, systems and controls; and

(c) monitoring internal reporting patterns.

PART 7

RECORD KEEPING

Meaning of "records"

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

Manner in which records to be kept

36. (1) A service provider shall ensure that its records are kept in such manner that—

(a) facilitates ongoing monitoring and their periodic updating;

(b) ensures that they are readily accessible to the service provider in Anguilla; and

(c) enables the Commission, internal and external auditors and other competent authorities to assess the effectiveness of policies, procedures, systems and controls that are maintained by the service provider to prevent and detect money laundering and the financing of terrorism.

(2) Where records are kept other than in legible form, they must be kept in such manner that enables them to be readily produced in Anguilla in legible form.

(3) A service provider shall ensure that the MLCO and other appropriate employees have timely access to all customer identification information records, other customer due diligence information, transaction records and other relevant information and records necessary for them to perform their functions.

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 period specified in section 20 of the Regulations, 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 5 years from the date a business relationship ends, or for 5 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 MLRO concerning whether to make a suspicious activity report to the Unit and the basis of that decision;

(c) details of any reports made to the 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 Unit for a period of at least 5 years from the date that the enquiry was made.

(R.A. 112/2022, s. 25)

Records concerning policies, procedures, systems and controls and training

39. (1) A service provider shall keep records documenting its policies, procedures, systems and controls to prevent and detect money laundering for a period of at least 5 years from the date that the policies, procedures, systems and controls are superseded or otherwise cease to have effect.

(2) A service provider shall keep records for at least 5 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 AML/CFT 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.

GUIDANCE

Introduction

(i) The principal reason for imposing record keeping requirements on service providers is to ensure that the law enforcement agencies in Anguilla 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 Anguilla 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 AML/CFT Regulations therefore impose certain record keeping requirements on service providers. These are summarised 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 AML/CFT 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 5 years from the date on which an occasional transaction is completed or the business relationship ends, or in the case of transaction records, 5 years from when the transaction is completed and for all other records, 5 years from the date on which the business relationship ends, unless the Commission 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 computerised or other electronic data;

(d) as scanned documents; or

(e) using a combination of the above.

PART 8

CORRESPONDENT BANKING AND SIMILAR RELATIONSHIPS

Restrictions on correspondent banking

42. An Anguilla bank that is, or that proposes to be, a correspondent bank shall—

(a) apply customer due diligence measures on respondent banks using a risk-based approach that enables the bank to fully understand the nature of the respondent bank's business and which takes into account, in particular—

(i) the respondent's domicile,

(ii) the respondent bank's ownership and management structure, and

(iii) the respondent bank's customer base, including its geographic location, its business, including the nature of services provided by the respondent bank to its customers, whether or not relationships are conducted by the respondent on a non-face-to-face basis and the extent to which the respondent bank relies on third parties to identify and hold evidence of identity on, or to conduct other due diligence on, its customers;

(b) determine from publicly available sources the reputation of the respondent bank and the quality of its supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;

(c) assess the respondent bank's anti-money laundering and terrorist financing systems and controls to ensure that they are consistent with the requirements of the FATF Recommendations;

(d) not enter into a new correspondent banking relationship unless it has the prior approval of senior management;

(e) ensure that the respective anti-money laundering and counter terrorist financing responsibilities of each party to the correspondent relationship are understood and properly documented;

(f) ensure that the correspondent relationship and its transactions are subject to annual review by senior management;

(g) be able to demonstrate that the information obtained in compliance with the requirements set out in this section is held for all existing and new correspondent relationships; and

(h) not enter into a correspondent banking relationship where it has knowledge or suspicion that the respondent or any of its customers is engaged in money laundering or the financing of terrorism.

Payable-through accounts

43. Where a correspondent bank provides customers of a respondent bank with direct access to its services, whether by way of payable-through accounts or by other means, it shall ensure that it is satisfied that the respondent bank—

(a) has undertaken appropriate customer due diligence and, where applicable, enhanced customer due diligence in respect of the customers that have direct access to the correspondent bank's services; and

(b) is able to provide relevant customer due diligence information and verification evidence to the correspondent bank upon request.

Other similar relationships

44. Sections 42 and 43 also apply to a financial business that—

(a) undertakes securities transactions or funds transfers on a cross-border basis;

(b) provides finance to facilitate international trade.

GUIDANCE

(i) Section 6(1) of the AML/CFT Regulations defines "correspondent banking relationship" as meaning a relationship that involves the provision of banking services by one bank, (the "correspondent bank") to another bank (the "respondent bank"). The term has this meaning in Part 8 of the Code.

A correspondent banking relationship enables the respondent bank to provide its own customers with the cross-border products and services that it cannot provide them with itself. In effect, the correspondent bank is an agent or intermediary for the respondent bank and provides services to the customers of the respondent bank. In most cases, Anguilla banks will be a respondent bank, rather than a correspondent bank.

(ii) Section 6(2) of the AML/CFT Regulations sets out a list of banking services included within the definition of correspondent banking as follows:

(a) cash management, including establishing interest-bearing accounts in different currencies;

(b) international wire transfers of funds;

(c) cheque clearing;

(d) payable-through accounts; and

(e) foreign exchange services.

Correspondent banking services can also include facilitating securities transactions and other services.

(iii) As a correspondent bank will usually have no direct relationship with the customers of the respondent bank, it will not usually be possible for it to verify their identities. Correspondent banks also usually have limited information regarding the nature of the underlying transactions, particularly when processing wire transfers or clearing cheques. Correspondent banking relationships must, therefore, be regarded as having a higher money laundering and terrorist financing risk attached to them.

(iv) Part 8 of the Code therefore specifies additional customer due diligence measures that must be applied to a correspondent banking relationship.

Payable-through accounts

(v) A payable-through account is an account through which a correspondent bank extends payment facilities or other services directly to the customers of the respondent bank.

(vi) Payable-through accounts pose additional AML/CFT risks to the correspondent bank and the Code therefore imposes additional obligations with respect to such accounts.

Other similar relationships

(vii) Although "correspondent banking relationship" is defined as a relationship between banks, other cross-border financial activities can pose a similar risk. Section 44 of the Code therefore requires a financial business (which is defined in section 1(1) of the AML/CFT Regulations) that engages in specified activities to comply with sections 42 and 43.

(viii) Although sections 42 and 43 of the Code apply to specific financial businesses, other financial businesses that are subject to similar risks should consider whether they should also apply sections 42 and 43 of the Code.

PART 9

WIRE TRANSFERS

Interpretation

45. For the purposes of this Part—

"batch file transfer" means several individual transfers of funds which are bundled together for transmission;

"full beneficiary information", with respect to a payee means—

(a) the payee's name;

(b) the payee's account number or, where the account number is not available, a unique identifier which allows the transaction to be traced back to the payee;

(R.A. 112/2022, s. 18(a))

"full originator information", with respect to a payer, means—

(a) the payer's name;

(b) the payer's account number or, where the account number is not available, a unique identifier which allows the transaction to be traced back to the payer; and

(c) one of the following—

(i) the payer's address,

(ii) the number of a government-issued document evidencing the payer's identity,

(iii) the payer's customer identification number,

(iv) the payer's date and place of birth;

(R.A. 112/2022, s. 18(b))

"intermediary payment service provider" means a payment service provider, neither of the payer nor the payee, that participates in the execution of transfer of funds;

(R.A. 112/2022, s. 18(c))

"payee" means a person who is the intended final recipient of transferred funds;

"payer" means a person who holds an account and allows a transfer of funds from that account or, where there is no account, a person who places an order for the transfer of funds;

"payment service provider" means a person whose business includes the provision of transfer of funds services;

"transfer of funds" means a transaction carried out on behalf of a payer through a payment service provider by electronic means with a view to making funds available to a payee at a payment service provider, irrespective of whether the payer and the payee are the same person;

"unique identifier" means a combination of letters, numbers or symbols determined by the payment service provider, in accordance with the protocols of the payment and settlement or messaging system used to effect the transfer of funds.

Scope of this Part

46. Subject to section 47, this Part applies to a transfer of funds in any currency which is sent or received by a payment service provider that is a financial business that carries on business in or from within Anguilla.

(R.A. 112/2022, s. 19)

Exemptions

47. (1) Subject to subsection (2), a transfer of funds carried out using a credit or debit card is exempt from this Part if—

(a) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services; and

(b) a unique identifier, allowing the transaction to be traced back to the payer, accompanies the transfer of funds.

(2) A transfer of funds is not exempt from the application of this Part if the credit or debit card is used as a payment system to effect a transfer of funds.

(R.A. 112/2022, s. 20(a))

(3) A transfer of funds made by mobile telephone or any other digital or information technology device is exempt from this Part if—

(a) the transfer is pre-paid and does not exceed $300; or

(b) each of the following applies—

(i) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services,

(ii) a unique identifier, allowing the transaction to be traced back to the payer, accompanies the transfer of funds, and

(iii) the payment service provider of the payee is a licensee.

(R.A. 112/2022, s. 20(c))

(4) A transfer of funds is exempt if—

(a) the payer withdraws cash from the payer's own account;

(b) there is a debit transfer authorisation between two parties permitting payments between them through accounts, provided a unique identifier accompanies the transfer of funds to enable the transaction to be traced back;

(c) it is made using truncated cheques;

(d) it is a transfer to the Government of, or a public body in, Anguilla for taxes, duties, fines or charges of any kind; or

(e) both the payer and the payee are payment service providers acting on their own behalf.

GUIDANCE

Introduction

(i) The purpose of this Part of the Code is to give effect in Anguilla to FATF Recommendation 16 concerning wire transfers.

(ii) FATF Recommendation 16 has the objective of enhancing the transparency of electronic payment transfers [commonly referred to as "wire transfers"] of all types, whether domestic or cross border, thereby making it easier for law enforcement agencies to track funds transferred electronically by money launderers, terrorists and other criminals.

(iii) A number of countries have put codes, rules or regulations in place to give effect to Recommendation 16. For example, in Europe, an EEC-wide Regulation came into effect on 1 January 2007. Although this Part of the Code ensures that Anguilla continues to comply with international standards, compliance with Recommendation 16 is also important to the financial sector in Anguilla because banks and payment service providers that fail to comply may in future find it difficult to send wire transfers to, or receive wire transfers from, countries that have given legal effect to FATF Recommendation 16.

(iv) In summary, this Part requires all payment service providers, as defined in the Code, to provide certain information in each wire transfer about the person who gives the instruction for the wire transfer to be made (the payer). Subject to a

number of permitted exemptions and variations, the information must always include the name, address and account number of the payer.

(v) However, the information does not have to be obtained and verified each time a customer requests a wire transfer; where the information had previously been obtained and verified and the entity effecting the transfer remains satisfied regarding the accuracy of the information on record, that information may be relied upon for subsequent transactions by the customer.

(vi) The application of this Part of the Code is subject to certain specified exemptions. These exemptions are transfers that present a very low risk for money laundering and terrorist financing.

Payment service provider of payer

48. (1) Subject to section 47, the payment service provider of a payer shall ensure that every transfer of funds is accompanied by the full originator payer information and the full beneficiary information.

(2) Subsection (1) does not apply in the case of a batch file transfer from a single payer, where some or all of the payment service providers of the payees are situated outside Anguilla, if—

(a) the batch file contains—

(i) the full originator information with respect to the payer, and

(ii) full beneficiary information in relation to the payee that is sufficient to enable traceability within the payee's country; and

(b) each of the individual transfers carries—

(i) the payer's account number or a unique identifier which allows the transaction to be traced back to the payer, and

(ii) the full beneficiary information in relation to the payee.

(3) The payment service provider of the payer shall, before transferring any funds, verify the full originator information and full beneficiary information on the basis of documents, data or information obtained from a reliable and independent source.

(4) In the case of a transfer from an account, verification referred to in subsection (3) with respect to the full originator information may be deemed to have taken place if—

(a) the account is held at a domestic bank or at a company that holds an offshore banking licence issued under the Trust Companies and Offshore Banking Act;

(b) the payer's identity has been verified in accordance with the applicable requirements of sections 18 to 24 of this Code; and

(c) information and documents relating to the verification of the payer have been kept and retained in accordance with section 19 of the AML/CFT Regulations.

(5) In the case of a transfer of funds not made from an account, the full originator information on the payer is deemed to have been verified by a payment service provider of the payer if—

(a) the transfer consists of a transaction of an amount not exceeding $2,500;

(b) the transfer is not a transaction that is carried out in several operations that appear to be linked and that together comprise an amount exceeding $2,500; and

(c) the payment service provider of the payer does not suspect that the payer is engaged in money laundering, terrorist financing or other financial crime.

(6) The payment service provider of the payer shall keep records of full originator information on the payer and full beneficiary information that accompanies the transfer of funds for a period of at least 5 years.

(7) Where the payment service provider of the payer and the payment service provider of the payee are both situated in Anguilla, a transfer of funds need only be accompanied by—

(a) the account number of the payee; or

(b) a unique identifier that allows the transaction to be traced back to the payer, where the payer does not have an account number.

(8) Where subsection (7) applies, the payment service provider of the payer shall, upon request from the payment service provider of the payee, make available to the payment service provider of the payee the full originator information within 3 working days, excluding the day on which the request was made.

(9) Where a payment service provider of the payer fails to comply with a request to provide the full originator information within the period specified in subsection (8), the payment service provider of the payee may notify the Commission which shall require the payment service provider of the payer to comply with the request immediately.

(10) Without prejudice to subsection (9), where a payment service provider of the payer fails to comply with a request, the payment service provider of the payee may—

(a) issue such warning to the payment service provider of the payer as may be considered necessary;

(b) set a deadline to enable the payment service provider of the payer to provide the required full originator information;

(c) reject future transfers of funds from the payment service provider of the payer; or

(d) restrict or terminate its business relationship with the payment service provider of the payer with respect to transfer of funds services or any mutual supply of services.

(11) A payment service provider of a payer shall not execute a transfer of funds if the requirements of this section are not complied with respect to the transfer.

(R.A. 112/2022, s. 21)

GUIDANCE

(i) One of the fundamental AML/CFT principles with respect to wire transfers, especially as they relate to cross-border batch transfers, is the timely provision

of full originator information by the payment service provider of the payer to the payment service provider of the payee when so requested. While it is acceptable to rely on oral requests in circumstances where there is assurance that the requested information would be provided within the specified period of three days after the date of the request, it is advisable that such requests be documented; this is particularly important for enforcement purposes where a request is not complied with as provided under this Code. Similarly, where the Commission is notified of a failure to accede to a request within the specified period, the Commission will issue a notice of requirement to comply under section 48(9) in writing. A record of regular or persistent breach on the part of a payment service provider of the payer would itself, where the payment service provider of the payer is licensed by the Commission, be a serious cause for concern and would be grounds for the Commission to take enforcement action against the payment service provider of the payer.

(ii) While routine batched wire transfers may not ordinarily present money laundering and terrorist financing risks, entities are required to adopt relevant measures to ensure that non-routine transactions are not batched in circumstances where doing so will or is likely to present such risks.

Payment service provider of payee

49. (1) The payment service provider of a payee shall take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify transfers of funds with any missing or incomplete—

(a) full originator information; or

(b) full beneficiary information.

(R.A. 112/2022, s. 22(b))

(2) In relation to a transfer of funds in an amount exceeding $2,500, the payment service provider of the payee shall verify the identity of the payee, if the identity has not been previously verified, and keep and retain the evidence of identity in accordance with section 19 of the AML/CFT Regulations.

(R.A. 112/2022, s. 22(b))

(3) A payment service provider of a payee shall establish and maintain risk-based policies and procedures for determining—

(a) when to execute, reject, or suspend a transfer of funds where the full originator information or the full beneficiary information is missing or incomplete; and

(b) the appropriate follow-up action.

(R.A. 112/2022, s. 22(c))

(4) Where the payment service provider of the payee becomes aware that the full originator information on the payer or the full beneficiary information with respect to a transfer of funds on the payee is missing or incomplete, the payment service provider of the payee shall—

(a) reject the transfer; or

(b) request for the full originator information on the payer and beneficiary information;

and, in either case determine whether and what follow-up action is appropriate.

(R.A. 112/2022, s. 22(c))

(5) Where a payment service provider regularly fails to supply the required information on the payer, the payment service provider of the payee shall adopt reasonable measures to rectify non-compliance with these Regulations, before—

(a) rejecting any future transfers of funds from that payment service provider;

(b) restricting its business relationship with that payment service provider; or

(c) terminating its business relationship with that payment service provider;

and the payment service provider of the payee shall report to the Commission and to the Unit any such decision to restrict or terminate its business relationship with that payment service provider.

(R.A. 112/2022, s. 22(c))

(6) A payment service provider of a payee shall not take action under subsection (4) or (5) if doing so would result in the payment service provider contravening a provision of the Act or the terrorist financing laws.

(R.A. 112/2022, s. 22(c))

(7) The payment service provider of a payee shall consider incomplete information about the payer as a factor in assessing whether the transfer of funds, or any related transaction, is suspicious, and whether the suspicion should be reported to the Unit as suspicious activity report.

(R.A. 112/2022, s. 22(c))

(8) The payment service provider of the payee shall keep records of any originator information on the payer and beneficiary information on the payee received for a period of at least 5 years.

(R.A. 112/2022, s. 22(c))

Intermediary payment service provider

50. (1) This section applies where the payment service provider of the payer is situated outside Anguilla and the intermediary payment service provider is situated within Anguilla.

(2) An intermediary payment service provider shall ensure that all originator and beneficiary information that accompanies a transfer of funds is kept with that transfer.

(R.A. 112/2022, s. 23(a))

(3) Where this section applies, an intermediary payment service provider, may use to send a transfer to the payment service provider of the payee, a system with technical limitations which prevents the required originator and beneficiary information from accompanying the transfer of funds.

(R.A. 112/2022, s. 23(b))

(4) Where, in receiving a transfer of funds, the intermediary payment service provider becomes aware that information on the payer or payee required under this Part is incomplete, the intermediary payment service provider may only use a payment system with technical limitations if the intermediary payment service provider (either through a payment or messaging system, or through another procedure that is accepted or agreed upon between the intermediary payment service provider and the payment service provider of the payee) provides confirmation that the information is incomplete.

(R.A. 112/2022, s. 23(c))

(5) An intermediary payment service provider that uses a system with technical limitations shall, if the payment service provider of the payee so requests, within 3 working days after the day on which the intermediary

payment service provider receives the request, make available to the payment service provider of the payee all the information on the payer that the intermediary payment service provider has received, whether or not the information is the full originator information.

(6) An intermediary payment service provider that uses a system with technical limitations which prevents the information on the payer from accompanying the transfer of funds shall keep records of all the information on the payer that it has received for a period of at least 5 years.

(7) An intermediary payment services provider shall take reasonable measures, consistent with straight through processing, to identify transfers of funds that lack full originator information or full beneficiary information.

(8) For the purposes of subsection (7), "straight through processing" means transfers of funds that are conducted electronically without the need for manual intervention.

(9) An intermediary payment services provider shall have risk-based policies and procedures for determining—

(a) when to execute, reject, or suspend a transfer of funds lacking full originator information or full beneficiary information; and

(b) the appropriate follow-up action.

(R.A. 112/2022, s. 23(d))

Money or Value Transfer Services Providers

51. (1) A money or value transfer services provider shall comply with all the relevant requirements of this Part in the countries in which it operates, whether directly or through its agents.

(2) A money or value transfer services provider that controls both the payment services provider of the payer and the payment services provider of the payee, shall—

(a) consider the information from both the payment services provider of the payer and the payment services provider of the payee to determine whether a suspicious activity report should be filed; and

(b) file a suspicious activity report or suspicious transaction report in the country from or to which the suspicious transfer of funds originated or was destined, respectively and make relevant transaction information available to the Unit and the relevant authorities in the country.

(R.A. 112/2022, s. 24)

PART 10

GENERAL

Citation

49. This Code may be cited as the Anti-Money Laundering and Terrorist Financing Code, Revised Regulations of Anguilla, P98-5.

———————

SCHEDULE

GUIDANCE ON ISSUES TO BE INCLUDED IN PROCEDURES MANUAL

This Schedule lists the issues that the Commission would normally expect to see included in a service provider's procedures manual. This Schedule is intended as guidance only. A service provider is responsible for ensuring that its procedures manual is comprehensive and appropriate. The list below should not, therefore, be considered to be exhaustive and it is not necessary for a service provider to cover the matters in the same order as presented in this Schedule.

1. Introduction of AML/CFT, KYC, CDD
   - (i) Define the terms above
   - (ii) Detail the purpose of the manual
   - (iii) Comment on Board of Director/Senior Management's commitment
2. AML – Procedures (Identifying Risks)
   - (i) Risk assessment (high, medium, low) say what policies are in place, explain the risk assessment process
   - (ii) Detail the responsibility of board (if any) for AML/CFT compliance
   - (iii) Outsourcing – policy and criteria for selection process
   - (iv) Responsibility of money laundering reporting officer
   - (v) Responsibility of money laundering compliance officer
3. KYC/Customer Due Diligence
   - (i) When is CDD obtained
   - (ii) Measures to be applied by service provider
   - (iii) Identification/verification information of individual clients
   - (iv) Identification/verification information on corporate entities
   - (v) Identification/verification of directors and beneficial owners
   - (vi) Identification/verification information, trusts and trustees
   - (vii) Identification/verification information foundations
4. Enhanced CDD
   - (i) Non face-to-face business
   - (ii) PEPs
   - (iii) Identification and approval process
5. Reliance on third parties
   - (i) Intermediaries and introducers
   - (ii) Documentation required
   - (iii) Certification required
   - (iv) Process of approval
6. Record keeping and training
   - (i) Transaction records - protection of data

(ii) Records containing suspicious transactions, activities, etc.

(iii) Records containing policies, procedures, systems and controls and training

(iv) Reviews of record keeping procedures

7. Reporting of suspicious transactions and activities

(i) What is a suspicious transaction or activity

(ii) Internal reporting procedures

(iii) MLRO reporting procedures

(iv) Evaluation of SARs by MLRO

(v) Reports to the Unit

(vi) Documenting SARs

8. Board/Senior Management approval of procedures

(R.A. 112/2022, s. 25)