

# Anguilla Financial Services Commission



## REPORT ON THEMED EXAMINATIONS PROGRAMME 2016 & 2017

*Anti-Money Laundering and Combating Financing of Terrorism  
Summary of Findings*

## TABLE OF CONTENTS

1	Introduction .....	1
2	Scope .....	1
3	Preliminary Observations .....	1
4	Areas of Substandard Performance .....	2
	4.1 Policies, Procedures, Systems and Controls .....	2
	4.2 Customer Due Diligence .....	2
	4.3 Risk Assessments (Business and Customer).....	2
	4.4 Enhanced Customer Due Diligence and Ongoing Monitoring .....	3
	4.5 Business Conducted Through Introducers and Intermediaries .....	3
5	Required Improvements .....	3
	5.1 Policies, Procedures, Systems and Controls .....	3
	5.2 Customer Due Diligence .....	4
	5.3 Risk Assessments (Business and Customer).....	6
	5.4 Enhanced Customer Due Diligence and Ongoing Monitoring .....	7
	5.5 Business Conducted Through Intermediaries and Introducers .....	9
6	Final Comments.....	10

## **1 Introduction**

- 1.1 In 2016 and 2017, the Anguilla Financial Services Commission (the “Commission”) continued its themed examinations to assess service providers’ compliance with the Anti-Money Laundering and Terrorist Financing (“AML/CFT”) legislation consisting of the Proceeds of Crime Act, R.S.A. c. P98 (“POCA”), AML/CFT Regulations, R.R.A, P98-1 (“AML/CFT Regulations”), AML/CFT Code, R.R.A. P98-3 (“AML/CFT Code”) and Externally and Non-Regulated Service Providers Regulations, R.R.A. P98-6 (“ENRSP Regulations”). Findings from these examinations as well as complaints made to the Commission evidence that there continue to be significant deficiencies in compliance by service providers with AML/CFT legislative requirements.
- 1.2 This report reviews areas where service providers’ performance is deficient and provides commentary on the specific improvements required. The Commission is releasing the Report to assist participants in the financial services industry to understand their obligations under AML/CFT legislation and to emphasize that the level of compliance by service providers with international standards not only impacts whether they meet the Commission’s fit and proper criteria to maintain a license but also has a direct bearing on the reputation, continued sustainability and growth of Anguilla’s financial services industry.

## **2 Scope**

- 2.1 The Commission’s 2016 and 2017 AML/CFT examination programme focused on company managers and externally regulated service providers (“service providers”).
- 2.2 Five (5) AML/CFT inspections were conducted between May and December 2016 and five (5) were conducted between February and August 2017. The Commission’s inspectors assessed whether service providers were compliant with the AML/CFT legislation. Inspectors reviewed and assessed service providers’ AML/CFT policies and procedures, staff training and awareness, suspicious activity reporting (“SARs”), appointment of money laundering reporting and money laundering compliance officers, and record keeping.
- 2.3 Prior to the inspection, the service providers completed a questionnaire that covered procedures relating to AML/CFT systems, controls and customer due diligence.
- 2.4 Inspectors reviewed, on a sample basis, the records, files and written policies and procedures maintained by the service providers and held discussions with management and staff involved in strategic, operational and compliance matters. A report was furnished for each service provider inspected. Where appropriate, specific areas for improvement were identified and deadlines set for remedial action by service providers.

## **3 Preliminary Observations**

- 3.1 The findings from the 2016 and 2017 examination programme evidence a number of areas that require increased vigilance and overall improvement of compliance with the AML/CFT legislation. These findings were especially evident in certain areas and the Commission intends to focus on those areas in this report - particularly in section 4 (areas of substandard performance) and section 5 (required improvements).

3.2 The Commission also strongly advises that practitioners review the AML/CFT Code, which is an excellent resource for AML/CFT compliance, easy to read with valuable guidance. The Code is a practical and useful document and can be used by practitioners for training of staff and in developing a framework for compliance with the AML/CFT legislation.

#### **4 Areas of Substandard Performance**

##### **4.1 Policies, Procedures, Systems and Controls**

4.1.1 All service providers inspected during 2016 and 2017 had an AML/CFT policies and procedures manual in compliance with section 16 of the AML/CFT Regulations and section 5 of the AML/CFT Code. The inspection team noted however, that in some cases significant policies and procedures were not documented. The noted policies and procedures were in relation to:

- the customer intake process;
- the collection of customer due diligence;
- conducting of the customer risk assessment;
- ongoing monitoring;
- enhanced due diligence;
- reporting suspicious activities;
- PEPs;
- introducers and intermediaries; and
- policies that identified countries lacking adequate AML laws, polices and compliance measures, high risk and non-cooperative jurisdictions or countries that do not or insufficiently apply the FATF Recommendations.

##### **4.2 Customer Due Diligence**

4.2.1 During the review of the sampled companies, in a few instances, some service providers failed to conduct sufficient customer due diligence measures in particular the failure to collect identification information and verification of identification information; proof of address documentation; source of wealth/source of funds information; and evidence to verify the nature of business. In many instances, the documents that were provided were uncertified. In addition, in some cases, copies of the documents proved illegible due to their poor quality.

##### **4.3 Risk Assessments (Business and Customer)**

###### **4.3.1 Business Risk Assessment**

4.3.1.1 A business risk assessment is the analysis of the overall risks faced by the service provider. Some of the service providers inspected did not have a documented risk assessment that is required under section 16(1) of the AML/CFT Regulations and section 3 of the AML/CFT Code. In some cases, a policy document was provided; a section of the AML/CFT Manual was allocated to the explanation of how a business risk assessment would be conducted; or nothing was provided at all. All of these instances do not satisfy the requirements of section 16(1) of the AML/CFT Regulations. Where a business risk assessment was conducted, an overall rating was not provided

and some important factors were not considered, particularly the nature of business conducted by its companies; business conducted through an intermediary; and delivery of the service providers' products and services.

#### **4.3.2 Customer Risk Assessment**

4.3.2.1 A customer risk assessment entails the assessment of the risk that a customer/company may be involved in or vulnerable to money laundering or terrorist financing. All service providers conducted customer risk assessments in accordance with section 10 of the AML/CFT Regulations and further elaborated on under section 10 of the AML/CFT Code, however, some companies were inaccurately risk rated given the nature of business identified.

#### **4.4 Enhanced Customer Due Diligence and Ongoing Monitoring**

4.4.1 The inspections highlighted that service providers failed to conduct sufficient ongoing monitoring on a regular basis. Since 2011, this has been a recurring issue. Reference is made to section 12 of the AML/CFT Regulations.

#### **4.5 Business Conducted Through Introducers and Intermediaries**

4.5.1 Generally, business conducted through introducers/intermediaries is considered high risk. In addition to not having adequate policies and procedures documented in its manual in relation to business conducted through an introducer/intermediary, service providers, in some cases, were unable to evidence that its intermediaries were regulated, supervised or monitored by a regulatory body for AML/CFT purposes. Furthermore, some service providers failed to test its regulated intermediaries on their awareness of the AML/CFT requirements in relation to customer due diligence and the responsiveness of its regulated intermediaries to requests for customer due diligence.

### **5 Required Improvements**

In relation to the identified areas of substandard performance, the Commission provides the following commentary to assist service providers to meet their obligations under AML/CFT legislation:

#### **5.1 Policies, Procedures, Systems and Controls**

5.1.1 All services providers must establish, maintain and implement appropriate risk-sensitive policies, systems and controls to prevent and detect money laundering and terrorist financing in accordance with section 16 of the AML/CFT Regulations. The policies, procedures, systems and controls established, maintained and implemented by a service provider must be documented in accordance with section 5 of the AML/CFT Code.

5.1.2 The inspection team notes that in some cases, service providers did not include procedures relating to the customer intake process and the collection of customer due diligence; customer risk assessment; ongoing monitoring; enhanced due diligence; reporting suspicious activities procedures; policies in relation to PEPs; introducers and intermediaries; and policies that identified countries lacking adequate AML laws,

policies and compliance measures, high risk and non-cooperative jurisdictions or countries that do not or insufficiently apply the FATF Recommendations.

- 5.1.3 Where such topics were included they were not adequately detailed. A mere regurgitation of the AML/CFT Regulations and the AML/CFT Code is not sufficient. A comprehensive procedures manual is an excellent ongoing reference source for employees and others, and may also be useful for staff training.
- 5.1.4 The procedures manual must be tailored for the service provider and its particular circumstances. By way of guidance, the procedures manual should normally include the issues and matters set out in the Schedule to the AML/CFT Code. The Commission has also included this guidance on its website (see link provided - <http://fsc.org.ai/documents/Document%20Library/Guidelines/AML-CFT%20Issues%20Guide%20for%20Procedures%20Manuals.pdf> )

## 5.2 Customer Due Diligence

### **5.2.1 Verification of Identification and Proof of Address documentation**

- 5.2.1.1 Undertaking customer due diligence measures is a statutory requirement for service providers reflected in section 10 of the AML/CFT Regulations and section 10 of the AML/CFT Code. The inspection team noted that in some cases, verification of identification information and proof of address documentation were not provided for the principals of a sample company. Where verification of identification information and proof of address documentation were provided, in some cases they were not certified.
- 5.2.1.2 Service providers must apply the customer due diligence measures outlined in sections 13 to 22 of the AML/CFT Code in relation to identification information and verification of identity of individuals, legal entities, trusts and trustees and foundations. The inspection team notes that in cases where a service provider has seen the original documentation, the service provider can certify the copies themselves following the procedures outlined in section 24 of the AML/CFT Code.
- 5.2.1.3 Where sufficient customer due diligence information has not been provided prior to the start of the business relationship and where a service provider cannot adequately assess the risk, a service provider should not enter into a business relationship with the customer. Additionally, if the company is an existing company, the service provider should resign. It may be determined that where insufficient customer due diligence has been collected, service providers cannot adequately risk rate its customers. In both cases where insufficient customer due diligence has been provided, the service provider should consider filing a suspicious activity report regardless if the service provider has begun a business relationship or not.
- 5.2.1.4 The inspection team noted that in some cases the quality of the customer due diligence was identified as deficient as some of the samples revealed poor quality copies that proved illegible. Service providers must ensure that during the collection of customer due diligence process, legible copies are made.

## **5.2.2 Relationship Information (Nature of Business)**

- 5.2.2.1 A necessary component of customer due diligence measures is the need to understand the nature of the customer's business and the transactions involved in order to correctly assess the money laundering and terrorist financing risk. This is detailed in the "relationship information" section found under section 11 of the AML/CFT Code.
- 5.2.2.2 In the Guidance following section 11 of the AML/CFT Code, item (xv) under "Relationship Information": *"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."*
- 5.2.2.3 While service providers may require a statement as to the intended nature of business at the time of incorporation, inspections have shown that service providers generally do not collect evidence to verify that the intended nature of business is still the present nature of business being carried out. Presently, service providers cannot effectively apply the necessary risk management measures, as the nature of business may not be what was initially stated and companies as a result may be incorrectly risk rated. As a result, service providers may not be applying the necessary customer due diligence measures commensurate with its risk (see section 5.3 on Customer Risk Assessment).
- 5.2.2.4 Service providers must verify the nature of business for all companies regardless of their risk rating. While brochures, business cards and a business plan may be collected at the start of the business relationship, a service provider may consider collecting on a regular basis information such as website screenshots, financial statements, invoices and bank statements; also conducting onsite visits where possible and making a note on its files about how the nature of business has been verified. The method used by the service provider will be dependent on its resources. Customers/companies should also be required to provide an update when there is a substantial change in the nature of business carried out.
- 5.2.2.5 Additionally, service providers should, but often did not, understand the structure of the customer's company. Evaluating the structure of the company requires an understanding of what the company is established to do and/or what the customer is trying to achieve. If there are unnecessary complexities in the corporate structure and unclear connections to entities incorporated in other jurisdictions, then service providers are required to investigate and determine valid business reasons for the complexity.

## **5.2.3 Relationship Information (Source of Funds/Source of Wealth)**

- 5.2.3.1 In addition to the nature of business, service providers are expected to collect from their customers 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.

5.2.3.2 The Commission's inspections evidenced that in some cases, source of funds information was not provided and in high risk rated companies, source of wealth information was not collected. Where the source of funds or source of wealth was identified, evidence was not provided that the service provider verified the information provided. Both the source of funds and source of wealth must be identified and verified.

### 5.3 Risk Assessments (Business and Customer)

#### 5.3.1 **Business Risk Assessments**

5.3.1.1 A service provider is required to carry out and document an overall business risk assessment. Where a service provider has not conducted an overall business risk assessment, the service provider cannot adequately assess the risks it faces and implement the appropriate safeguards against such risks making the service provider vulnerable to possible money laundering and terrorist financing risks.

5.3.1.2 A business risk assessment assesses the possible money laundering and terrorist financing risks that a service provider faces; determines how to best manage those risks identified; and helps the designing, establishing, maintaining and implementing of AML/CFT policies, systems and controls. However, before a service provider can conduct a business risk assessment, a service provider must ensure that all customer files and information are up to date and accurate and individual customer risk assessments have been conducted on all of its customers (see section 5.3.2 on Customer Risk Assessments). This information provides the foundation for the business risk assessment analysis of the below categories.

5.3.1.3 A service provider will not be able to demonstrate an effective and thorough assessment of the AML/CFT risks/vulnerabilities faced by the service provider without evaluating at least the following categories:

- a. Customer base/type of customers and the nature of business conducted by its customers; e.g. PEPs, high value dealers, local residents;
- b. Products and services offered, e.g. incorporation, nominee shareholder, secretarial services;
- c. Delivery of its products and services, e.g. face-to-face; non face-to-face; the use of third parties, i.e. intermediaries; and
- d. Geographical location of customers, e.g. high-risk jurisdictions, well-regulated jurisdictions.

5.3.1.4 Each category should be rated as either high, medium or low risk. In addition, an overall risk rating should be given. The Commission notes that service providers have not been collecting sufficient information on the nature of business of its companies. In addition, service providers have been focusing on where the beneficial owners are located and not where the companies' business is being conducted and who the company trades with. Therefore, the customer base and geographical risks of the business risk assessment would be inaccurate.

5.3.1.5 A service provider should also highlight the internal controls and policies that have been implemented to counter its risks. This should include a strategic plan that commits

resources for AML/CFT staffing and training and periodic reviews and updating of the business risk assessment if there are material changes to the categories outlined above.

### 5.3.2 Customer Risk Assessments

5.3.2.1 Customer Risk Assessments are necessary to assess the risk that a customer/company may be involved in money laundering or terrorist financing. An adequate customer risk assessment entails the service provider knowing all aspects of each of its companies. While the Commission notes that service providers are generally good at collecting identification information, verification of identification information and proof of address documents, there has been a deficiency in collecting evidence to verify the nature of business and the monitoring of companies' nature of business conducted.

5.3.2.2 The inspectors noted that in some cases, customer risk assessments carried out were erroneous as the service provider failed to recognize that the nature of business the company initially stated was not the nature of business being carried out currently.

5.3.2.3 In some cases, the examiners noted that service providers considered manufacturing, trading, capital movement investment and technology as low risk activities. The Commission notes that such industries are considered to be cash intensive and therefore represent a high risk of money laundering. The Commission draws to the service providers' attention the Guidance following the Relationship Information (section 11) of the AML/CFT Code ("Guidance"), clause (xx)(c) under the customer risk section that states that, "*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.*" Where a company is inadequately risk rated, the service provider would be unlikely to apply the appropriate risk management measures.

5.3.2.4 A service provider must periodically update its customer risk assessments in relation to the risk rating assigned (see section 5.4 on Enhanced Customer Due Diligence and Ongoing Monitoring).

### 5.4 Enhanced Customer Due Diligence and Ongoing Monitoring

5.4.1 Service providers are reminded that it must apply enhanced due diligence measures and in addition to normal on going monitoring efforts, undertake enhanced ongoing monitoring in accordance with section 12 of the AML/CFT Regulations in all cases where a customer is assessed as high risk. This is to include but is not limited to situations where customers were incorporated through an intermediary; non face to face business is conducted; the company is engaged in a cash intensive business; and the involvement of PEPs.

5.4.2 It must be emphasized that ongoing monitoring is the sole responsibility of the service provider. Ongoing monitoring is defined in section 4(5) of the AML/CFT Regulations as the scrutinising of 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 undertaking reviews of existing records; and 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.”.*

- 5.4.3 The inspection team noted that missing customer due diligence information and evidence and expired IDs, were found during its sample file review. In order to properly conduct ongoing monitoring licensed serviced providers should also have the necessary up-to-date contact information on file. This should include email addresses and/or telephone numbers for all principals of the company in order to gather the required information.
- 5.4.4 In addition, as noted above, service providers did not sufficiently verify the nature of business and failed to undertake ongoing monitoring to determine whether the business activity is the same as previously stated. The inspection team found that as a result, in some cases, the nature or purpose of one or more of their customers’ businesses, as represented by the customer, differed significantly from the actual business being conducted. This was significantly highlighted where the Commission found that non-regulated investment business i.e. forex and binary option trading, was taking place. This is disturbing and certainly shows that service providers have failed to conduct ongoing monitoring. Service providers are reminded that it must understand the nature of business engaged in by its customers that can only be truly achieved if the correct nature of business is known and ongoing monitoring of the nature of business is conducted.
- 5.4.5 Service providers are to document their ongoing monitoring procedure in its manual. The procedure should include the frequency of reviews of customer files in relation to the risk associated with the customer. The frequency of the reviews/updates can also be impacted by factors such as unusual customer profiles; new business relationships; higher risk business; and sanction regimes affecting other countries.
- 5.4.6 If during a review, a customer is reassessed to be high risk, enhanced due diligence measures and enhanced ongoing monitoring procedures in accordance with section 12 of the AML/CFT Regulations must be applied. See *Guidelines For Conducting Company Management Business Directly Or Through An Intermediary In Compliance With AML/CFT Legislation* published on the Commission’s website (see link provided - [http://fsc.org.ai/documents/Document%20Library/Guidelines/Guidelines%20for%20the%20Conduct%20of%20Company%20Management%20Business%20Through%20an%20Intermediary\\_Revised\\_31.10.2017.pdf](http://fsc.org.ai/documents/Document%20Library/Guidelines/Guidelines%20for%20the%20Conduct%20of%20Company%20Management%20Business%20Through%20an%20Intermediary_Revised_31.10.2017.pdf) ).

#### 5.4.7 **Politically Exposed Persons**

- 5.4.7.1 The inspection team noted that in some cases, the list of PEPs was not regularly reviewed and amended. Service providers must ensure that it regularly reviews and updates its PEP list. Google searches, newspaper articles, social media, commercial databases, government issued PEP lists and customer self-declarations are all ways in which service providers can determine whether any of their customers are a PEP. Service providers should also be aware that non-PEPs may become PEPs later in the business relationship and therefore the regular monitoring of customer profiles and

account activity is important in addition to the review of the suggested sources listed above.

## 5.5 Business Conducted Through Intermediaries and Introducers

- 5.5.1 In some cases, service providers did not have documented policies and procedures on conducting business with introducers/intermediaries, including where reliance was placed on those third parties. Service providers must be able to evidence that their Board of Directors reviewed and approved policies and procedures for conducting business with introducers and intermediaries. Such policies and procedures should be included in the AML/CFT Manual so that staff is familiar with the process.
- 5.5.2 The inspection team noted that service providers relied on the fact that intermediaries were members of professional associations. Although these intermediaries may be subject to professional rules and codes of conduct, there was no evidence provided to indicate that the intermediaries were actively regulated for AML/CFT purposes. Where there is no evidence that the intermediaries are actively regulated for AML/CFT purposes, a service provider cannot rely on its intermediaries to apply customer due diligence measures in accordance with section 13(1) of the AML/CFT Regulations. In such cases, the service provider must hold all customer due diligence information and evidence.
- 5.5.3 Service providers must be aware of the procedures that its intermediaries use to conduct their business, including whether the intermediaries meet the customers face to face.
- 5.5.4 Service providers are reminded to enter into an agreement with any introducer/intermediary upon which they place reliance (i.e. a regulated introducer/intermediary). The agreement must detail the obligations of the introducer/intermediary to provide required due diligence information, both pre-incorporation and, if applicable, to enable the service provider to conduct effective ongoing monitoring. In some cases, the inspection team noted that some of the agreements were not signed by both parties. Service providers should ensure that the agreements are reviewed and signed by both parties. Agreements should also be updated regularly where there are changes in AML/CFT legislation and obligations.
- 5.5.5 Service providers should be testing its intermediaries' responsiveness to requests for customer due diligence and the quality of customer due diligence provided. The Commission expects, in cases where there is a consistent pattern displayed by an intermediary of slow responses; poor quality of customer due diligence information; and problematic customers, that the relationship be terminated. The Commission reminds service providers that they, and not the intermediary, are liable under AML/CFT legislation for a failure to conduct appropriate customer due diligence.
- 5.5.6 Conducting business through an intermediary is considered non face to face business and is therefore considered to be high risk. Service providers must conduct enhanced due diligence in all cases where customers were not met face to face. Reference is made to the *Guidelines For Conducting Company Management Business Directly Or Through An Intermediary In Compliance With AML/CFT Legislation* (see section 5.4 on Enhanced Customer Due Diligence and Ongoing Monitoring).

## **6 Final Comments**

- 6.1 The Commission notes that there is a need for a clearer understanding of the AML/CFT Legislation and the responsibilities outlined within it by all service providers. The focus has shifted from the mere incorporation and sporadic monitoring of companies to the requirement for service providers to collect more information; conduct additional checks; engage in regular ongoing monitoring; and applying enhanced ongoing monitoring and enhanced due diligence measures where necessary. Therefore, service providers must be more active and committed in fulfilling its AML/CFT obligations.
- 6.2 Service providers are only able to apply the necessary customer due diligence measures and risk mitigation measures where it is familiar and understands all aspects of all companies in its portfolio.
- 6.3 Particular emphasis should be placed on knowing the structure of the company and the nature of transactions carried out within the company. Only then will a service provider be able to determine the risk rating to be assigned; the level of customer due diligence measures to be applied; and whether enhanced ongoing monitoring and enhanced due diligence measures are required. Without a proper understanding of the companies in which it manages, service providers are vulnerable to money laundering and terrorist financing risks and enforcement measures by the Commission.
- 6.4 Service providers must adequately monitor its companies on a regular basis for changes that could affect the way in which the company is to be monitored. In order to do this, sufficient information must be collected from the customer.

Approved by the Board  
**Anguilla Financial Services Commission**  
14 March 2019