Anti-Money Laundering (AML) & Counter Terrorism Financing (CTF) Policy and Procedures

Version: 01-01052019

Contents

1. INTRODUCTION

1.1 Rational

Infinox Capital ("Infinox")is a registered trading name of IX Capital Group Limited ("IXCG), a company duly incorporated under the law of the Commonwealth of The Bahamas and regulated by the Securities Commission of The Bahamas ("SCB"). We are authorized by the SCB to deal, arrange and manage securities. The Firm is committed to complying with its legal and regulatory responsibilities in relation to Anti-Money Laundering & Counter Terrorist Funding (AML/CTF) and has no appetite for non-compliance.

The Anti-Money Laundering & Counter Terrorist Financing Policy (the "AML/CTF" Policy) is a mandatory requirement for the Firm and applies to all employees (temporary and permanent) in all jurisdictions where the company operates.

The Policy clearly articulates a set of minimum standards and requirements that meet and aim to exceed regulatory and legislative obligations and the guidance provided by the SCB.

1.2 Applicable Regulation

This AML/CTF policy ensures it addresses and incorporates the regulatory requirements set out in the below applicable regulation.

The Firm is subject to the laws of The Bahamas and rules set by the SCB. The SCB provides practical interpretation of legal and regulatory requirements and indicates good industry practice. The Firm has taken these laws and guidelines in to account when devising a risk-based approach to the prevention of money laundering.

The laws of The Bahamas specifically concerning money laundering and terrorist financing is contained in the following legislation:

- the Proceeds of Crime Act, 2018 ("POCA") (as amended);
- the Anti-Terrorism Act, 2018 (as amended);
- the Financial Transactions Reporting Act, 2018 (as amended) ("FTRA");
- the Financial Transactions Reporting Regulations, 2018 (as amended) ("FTRR");
- the Financial Transactions Reporting (Wire Transfers) Regulations, 2009;
- the Financial Intelligence Unit Act, 2000 (as amended) ("FIUA");
- the Financial Intelligence (Transactions Reporting) Regulations, 2001 (as amended);
- the Securities Industry Act, 2011 (as amended) ("SIA"); and,
- the Securities Industry (Anti Money Laundering and Countering the Financing of Terrorism) Rules, 2015 (as amended) ("SIR")

1.3 Purpose of this AML/CTF Policy

This AML/CTF policy has been prepared so that Firm can assess the potential money laundering and terrorist financing ("AML/CTF") risks to which it may be exposed and to manage those risks within the legislative framework. The policy demonstrates the extent of Firm's Client Due Diligence ("CDD") measures − that it is comprehensive, proportionate and appropriate to the nature, scale and complexity of Firm's activities in light of the risks of money laundering and terrorist financing facing the business.

The Firm˚s AML/CTF policy was updated in May, 2019. These policies are reviewed annually or as often as necessary.

This policy is separated into two parts:

1) The primary purpose of Part 1 of this AML/CTF Policy is to provide a background into Money Laundering and its regulation, and also how to identify, mitigate and manage the risk that the Firm may reasonably face (inadvertently or otherwise) by facilitating money laundering or terrorism financing through the regulated activities it undertakes.
2) Part 2 of the AML/CTF policy goes into the detail of the Firm˚s customer identification and verification procedures, enhanced due diligence measures, country risk ratings, Politically Exposed Persons and so forth.

Through its policies, procedures and compliance culture, the Firm ensures that it has adequate internal controls and monitoring systems in place to mitigate against the risk of money laundering or terrorist financing. These should alert all relevant people if criminals attempt to use the business for money laundering.

2. BACKGROUND

2.1 What is Money Laundering?

Money laundering is the generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source.

The processes by which criminally derived property may be laundered are extensive. Though criminal money may be successfully laundered without the assistance of the financial sector, the reality is that hundreds of billions of dollars of criminally derived money is laundered through financial institutions, annually. The nature of the services and products offered by the financial services industry (namely managing, controlling and possessing money and property belonging to others) means that it is vulnerable to abuse by money launderers.

2.2 How is an Offence Committed?

Money laundering offences have similar characteristics globally. There are two key elements to a money laundering offence:

1) A requisite degree of knowledge or suspicion (either subjective or objective) relating to the source of the funds or the conduct of a client; and,
2) The act of laundering is committed in circumstances where a person is engaged in an arrangement (i.e. by providing a service or product) and that arrangement involves the proceeds of crime. These arrangements include a wide variety of business relationships (i.e. banking, fiduciary and investment management).

The requisite degree of knowledge or suspicion will depend upon the specific offence but will usually be present where the person providing the arrangement, service or product knows, suspects or has reasonable grounds to suspect that the property involved in the arrangement represents the proceeds of crime. In some cases, the offence may also be committed where a person knows or suspects that the person with whom he or she is dealing is engaged in or has benefited from criminal conduct.

2.3 How is Money Laundered?

The processes are extensive. Money is laundered whenever a person or business deals in any way with another person˚s benefit from crime. That can occur in a countless number of diverse ways.

Traditionally, money laundering has been described as a process which takes place in three distinct stages.

1) Placement, the stage at which criminally derived funds are introduced in the financial system.
2) Layering, the substantive stage of the process in which the property is ˛washed˚ and its ownership and source is disguised.
3) Integration, the final stage at which the ˛laundered˚ property is re-introduced into the legitimate economy.

This three-staged definition of money laundering is highly simplistic. The reality is that the so-called stages often overlap and in some cases, for example in cases of financial crimes, there is no requirement for the proceeds of crime to be ˛placed˚.

3. FINANCIAL CRIME

3.1 Money Laundering Risk

This is the risk that a Firm may be used to further money laundering. Failure by a Firm to manage this risk effectively will increase the risk to society of crime and terrorism.

Money Laundering takes many forms, including:

- trying to turn money raised through criminal activity into ˛clean˚ money (that is, classic money laundering);
- handling the benefit of acquisitive crimes such as theft, fraud and tax evasion; handling stolen goods;
- being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property; and,
- criminals investing the proceeds of their crimes in the whole range of financial products.

There are three broad groups of offences related to money laundering that the Firm needs to avoid committing. These are:

1) Knowingly assisting (in many specified ways) in concealing, or entering into arrangements for the acquisition, use, and/or possession of, criminal property;
2) Failing to report knowledge, suspicion, or where there are reasonable grounds for knowing or suspecting, that another person is engaged in money laundering; and,
3) Tipping off or prejudicing an investigation.

3.2 Terrorist Financing Risk

This is the risk that a Firm may be used to aid the activities by financing of terrorist groups or individuals. There can be considerable similarities between the movement of terrorist property and the laundering of criminal property: some terrorist groups are known to have well established links with organised criminal activity. However, there are two major differences between terrorist property and criminal property more generally:

- Often only small amounts are required to commit individual terrorist acts, thus increasing the difficulty of tracking the terrorist property;

- Terrorists can be funded from legitimately obtained income, including charitable donations, and it is extremely difficult to identify the stage at which legitimate funds become terrorist property.

3.3 Regulatory Obligations

1) The Firm must have systems and controls to identify, assess and monitor money-laundering risk as well as Client Due Diligence (‘CDD’) measures and monitoring to manage the risks identified.
2) In combating terrorist financing, the obligation on the Firm is to report any suspicious activity to the Financial Intelligence Unit (‘FIU’).
3) This supports the aims of the law enforcement agencies in relation to the financing of terrorism, by allowing the freezing of property where there are reasonable grounds for suspecting that such property could be used to finance terrorist activity, and depriving terrorists of this property as and when links are established between the property and terrorists or terrorist activity.
4) The Firm is required to determine the extent of CDD measures and monitoring on a risk-sensitive basis depending on the type of customer, business relationship and product or transaction.

4. LAWS AND REGULATIONS

4.1 Introduction

There are a number of pieces of legislation that make up the Anti Money Laundering and Counter Terrorist Financing framework. A summary of the main pieces of legislation is provided in Appendix 6. All employees of the Firm should be aware that it is not only the Firm that is subject to the legislation but also the employees within the firm. Failure to comply with certain aspects of the legislation can result in an individual being subject to prosecution with the threat of a custodial sentence or fine.

4.1 Proceeds of Crime Act, 2018

The Proceeds of Crime Act, 2018, (‘POCA’) is the main piece of legislation dealing with individual criminal liability in relation to money laundering. Offences under POCA occur in relation to criminal conduct and/or criminal property and punishable by imprisonment and fines.

4.2 Money Laundering

The Act provides that a person is guilty of the offence of money laundering if he uses, transfers, sends or delivers to any person or place any property which, in whole or in part directly or indirectly represents proceeds of criminal conduct; or disposes of, converts, alters or otherwise deals with that property in any manner and by any means with the intent to conceal or disguise such property.

A person is also guilty of money laundering if he knows, suspects or has reasonable grounds to suspect that any property in whole or in part directly or indirectly represents another person’s proceeds of criminal conduct and he uses, transfers, sends or delivers to any person or place that property; or disposes of or otherwise deals with in any manner by any means that property, with the intent to conceal or disguise the property.

Section 11 of the Act provides inter alia that it is an offence for a person to assist another to retain or live off the proceeds of criminal conduct knowing, suspecting, or having reasonable grounds to suspect that the other person is or has been engaged in or has benefited from criminal conduct.
It is a defence for a person to prove that he or she did not know, suspect or have reasonable grounds to suspect that:

a) the arrangement in question related to any person˙s proceeds of criminal conduct; or
b) the arrangement facilitated the retention or control of any property by or on behalf of the suspected person; or
c) by arrangement any property was used as mentioned in (b).

The Act provides that a person is guilty of an offence if he knows, suspects or has reasonable grounds to suspect that any property in whole or in part directly or indirectly represents, another person˙s proceeds of criminal conduct, and he acquires or uses that property or has possession of it.

4.3 Failure to Disclose Suspicious Transactions

It is an offence for a person who knows suspects or has reasonable grounds to suspect that another person is engaged in money laundering, which relates to any proceeds of drug trafficking or any relevant offence, to fail to disclose this to the Financial Intelligence Unit or to a police officer.

A person is also guilty of an offence where the information, or other matter, on which his knowledge or suspicion is based came to his attention in the course of his trade, profession, business or employment and he fails to disclose the information or other matter to a police officer as soon as is reasonably practicable after it comes to his attention.

4.4 Tipping Off

It is a criminal offence under POCA to take action likely to prejudice an investigation by informing (tipping off) the subject of a suspicious report, or anyone else, that a disclosure has been made to either the FIU or the MLRO or that the police or customs authorities are carrying out or intending to carry out a money laundering investigation.

It is an offence to disclose information that is likely to prejudice an investigation if the person knows, suspects or has reasonable grounds to suspect that an investigation into money laundering is being, or is about to be, conducted or if he knows, suspects or has reasonable grounds for suspecting that a disclosure has been made.

4.5 Destruction of Documents

It is an offence under POCA to destroy or dispose of documents that may be relevant to a money laundering investigation.

4.6 Anti-Terrorism Act, 2018

The Anti-Terrorism Act, 2018, (as amended) establishes offences related to involvement in facilitating, raising, possessing or using funds for terrorism purposes, failing to report, tipping off or prejudicing an investigation.

The Act makes it a criminal offence for any person not to report the existence of terrorist property where there are reasonable grounds for knowing or suspecting the existence of terrorist property. It is also a criminal offence for anyone to take any action likely to prejudice an investigation by informing (i.e. tipping off) the person who is the subject of a suspicion report, or anybody else, that a disclosure has been made to a MLRO or to the FIU, or that the police or customs authorities are carrying out or intending to carry out a terrorist financing investigation.

The Act grants a power to the law enforcement agencies to make an account monitoring order, similar in scope to that introduced under POCA.

Failure to report is punishable by imprisonment and fines.

The Act gives the authorities power to direct firms in the regulated sector to provide the authorities with specified information on clients and their terrorism-related activities.

4.7 The Financial Transactions Reporting Act, 2018

The Financial Transactions Reporting Act, 2018, mandates that financial institutions verify the identity of their customers.

The Act provides that an offence is committed where a financial institution:

a) permits a person to become a facility holder in relation to any facility without having first verified the identity of that person;
b) permits any person to conduct an occasional transaction in excess of $15,000.00 without first having verified the identity of that person;
c) fails to verify the identity of a person conducting an occasional transaction as soon as practicable after the conditions have been satisfied in respect of that transaction;
d) fails to verify the identity of a person on whose behalf an occasional transaction in excess of $15,000.00 is being or has been conducted;
e) fails to undertake the verification required in relation to persons conducting an occasional transaction in excess of 15,000.00 in circumstances where it reasonably appears that the transaction is being conducted on behalf of any other person or persons and that the transactions are or have been structured to avoid verification of identity;
f) fails, before a transaction is conducted, to verify the identity of a person on whose behalf a facility holder is conducting a transaction in excess of $15,000.00 that where it has reasonable grounds to believe circumstances exist; and
g) fails to undertake the verification required.

The Act makes it mandatory for a financial institution to report to the FIU any transaction conducted by, through or with a financial institution or any proposed transaction (whether or not the transaction involves funds) where the financial institution knows, suspects or has reasonable grounds to suspect that the transaction or proposed transaction involves proceeds of criminal conduct as defined in the Proceeds of Crime Act, 2018, or any offence under the Proceeds of Crime Act, or in attempt to avoid the enforcement of any provision of the Proceeds of Crime Act.

4.8 Penalty for Failing to Report Suspicious Transactions

A Financial institution who contravenes these provisions is liable to imprisonment for a term of up to five years or to a fine of up to five hundred thousand dollars or to both.

4.9 US Legal Obligations

Even though FIRM does not accept US residents as clients, the US criminal money laundering laws, in particular the USA Patriot Act 2001 (as amended), have an extra-territorial effect. Where FIRM deals in the US Dollar or maintains banking relationships there is a risk that US regulations and sanctions may apply.

5. MONEY LAUNDERING REPORTING OFFICER

5.1 Internal Communications

The Money Laundering Reporting Officer (ʻMLROʼ) the Firmʼs designated employee with the overall responsibility for the establishment and maintenance of effective anti-money laundering systems and controls.

The MLRO is a required function which requires regulatory approval of that person. The regulator expects the MLRO to be based in The Bahamas and to be of sufficient seniority within Firm to be able to act on his/her own authority. The MLRO must have access to all Know Your Business information.

The MLROʼs responsibilities include the following:

1) Monitoring of the effectiveness of the Firmʼs anti-money laundering controls;
2) Overseeing the firmʼs compliance with the regulatorʼs rules on anti-money laundering systems and controls;
3) Having overall responsibility for the day-to-day operation of such policies, even where these have been delegated;
4) Ensuring that client acceptance standards are compliant with the Firmʼs policies;
5) Receiving and reviewing internal disclosures and submitting external reports to the FIU;
6) Responding promptly to any reasonable request for information made by the Central Bank of The Bahamas, SCB, FIU or law enforcement;
7) Liaising with the SCB, the FIU and other external agencies;
8) Ensuring that anti-money laundering training is provided, its standards and scope are appropriate and that records are kept;
9) Reporting to the Board on at least an annual basis (via a MLRO Report) and keeping the management updated on money laundering issues;
10) Obtaining and using national and international findings, for example the findings of the FATF, IMF and World Bank;
11) Appointing of a Deputy MLRO to cover the MLROʼs periods of absence (if the MLRO is temporarily unavailable for 12 weeks or more in any consecutive 12-months period, regulatory pre-approval is required);
12) Ensuring that the client and transaction monitoring is being undertaken;
13) Assessing the risks of the Firmʼs client base and business activities in relation to money laundering on an on-going basis; and
14) Ensuring the firmʼs policies and procedures are being communicated effectively to all relevant employees.

While the MLRO may delegate their duties to another appropriate person, such delegation needs to be documented. In such cases the regulator will expect the MLRO to take ultimate managerial responsibility.

5.2 Contact with Third Parties

The Firmʼs personnel must not discuss any issues relating to the Firmʼs anti-money laundering policies and procedures with any third parties without prior consent of the MLRO. All requests from the regulator or other investigating and enforcement agencies must be referred to the MLRO without delay.

5.3 Court Orders

The following orders may be served on the Firm as part of an on-going investigation. Should you receive any such order, please give it to the MLRO without delay:

- a production order;
- a disclosure order;
- a client information order;
- an account monitoring order;
- a search and seizure warrant; or
- an order for financial information under an Act

6. RISK-BASED APPROACH

6.1 Introduction

The Firm is required to operate a risk-based policy in order to identify, manage and mitigate the risks associated with the Firm being used for money laundering or terrorist financing. This approach will identify the most cost effective and proportionate way to manage and mitigate the risks posed to Firm. It is accepted that a risk based regime cannot be a zero-failure regime but that it should strike a balance between cost and the realistic threat of being used for money laundering or terrorist financing. The aim is to focus the efforts where they are most needed and will have most impact.

A risk based approach requires Firm to undertake the following steps:

1) Assess the risks applicable to the Firm. The Firm recognizes that the money laundering risks predominately posed to the Firm are due to the nature that the services are offered on an on-line basis which means that our clients are accepted on a non-face-to-face basis;
2) Allows the MLRO and / or the board to design and implement controls to manage and mitigate these risks;
3) Assist, monitor and improve the effective operation of the Firm˝s controls in a cost-effective way;
4) Reduce risks wherever and whenever possible; and,
5) To promote the prioritization of effective group policy and to record what has been done and why.

6.2 Regulatory Permissions

The Firm is authorised and regulated by SCB, and the Firm˝s scope of permissions relate to:

- Dealing in securities
- Arranging deals in securities
- Managing securities

6.3 Risk Potential

The Firm counters and mitigates the money laundering risk in a number of ways, including:

- Client identification standards based on client jurisdiction
- No cash dealings
- No acceptance of third-party payments
- Restrictions on transactions from higher risk countries
- Unless otherwise approved by the MLRO, all funds are paid back to the original bank account from which they were received.

6.4 Evaluating Risks

The Firm adopts a risk-based approach to business that enables it to utilise its resources in the most efficient and cost-effective manner. While the Firm will, as far as reasonably practicable, ensure consistent application of our risk-based approach, we recognise that this approach cannot anticipate every eventuality. Therefore, in any given case the MLRO may exercise his/her judgment in deciding whether or not to deviate from the written policies. This judgment will be clearly reasoned and documented.

In devising and implementing a risk-based approach, The Firm considers the following major risks. These risks are further discussed throughout this Manual.

1) Non-face-to-face Business

The Firm undertakes broker-dealer activities with individual retail clients who reside in any number of countries throughout the world on a non-face-to-face basis. As the Firm conducts its regulated activities on a non-face-to-face basis there is an increase in the risk of money laundering to the Firm. This risk may be mitigated by applying one or more of the following practices:

- requiring the customer's first payment or transaction to be carried out through an account in the customer's name with a Bahamian financial institution or a financial institution located in a country listed in the First Schedule to the FTRA;
- requiring additional documents to complement those required for face-to-face customers; (c) making telephone contact with the customer on a home or business number which has been verified prior to opening an account or conducting a transaction;
- communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, might be required to be returned completed or acknowledged without alteration);
- 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
- requiring copy documents to be certified by a suitable certifier.

Any subsequent change to the client's name, address, or employment details of which the Licensee becomes aware should be recorded and be regarded as a 'trigger' event. Generally, a KYC review would be undertaken as part of good business practice and due diligence process but it would also serve for money laundering or terrorist financing prevention.

2) Delivery channels for payment for services

In the normal course of business the Firm expects to receive funds electronically. Therefore, it would be highly unusual for us to receive cash payments. The electronic method identifies the sender and the record is verified against the account holder. Therefore, payments from unconnected third parties would be automatically returned to the remitter immediately.

3) Geographical location of the client and their business

It is possible for the Firm to deal with clients in other jurisdictions. However, clients resident in higher risk jurisdictions will be identified in accordance with Firm's risk based approach. Any factors mitigating the jurisdictional risk of the client must be documented. This may be the case when a

company has legitimate commercial interests in a high-risk jurisdiction and we understand the reasons for this company using our services.

6.5 Controls

Controls to mitigate risks include:

- Appointing a Money Laundering Reporting Officer (ʺMLROʺ);
- and making sure that all employees know how, why and where to report any suspicious activity;
- Identifying the responsibilities of senior managers and providing them with regular information on money laundering risks;
- Training relevant employees on their anti-money laundering responsibilities;
- Documenting anti-money laundering policies and procedures; and
- Introducing measures to make sure that the risk of money laundering is taken into account in the day-to-day running of the business.

6.6 Risk Factors

The Firmˆs primary mode of operation is by way of an electronic trading platform which operates over the Internet (i.e. the Firm gives clients direct online access to the rates/prices in the derivatives and foreign exchange markets at which the Firm is prepared to deal).

As a result, the Firm has considered the following risk posed by the following factors:

- Where the prospective customer (natural person, director, beneficiary or beneficial owner) is named in a government list or a credible sourceˆs list (sanctions lists) as identified by reporting services;
- Where the risk of terrorism is identified;
- Where the customer, who is an individual (natural person), is a Politically Exposed Person (ʺPEPʺ) or is known to have a link to a PEP (domestic or foreign); enhanced due diligence will be applied to any PEPs;
- Where a non-natural person (i.e. not a human) is a PEP or is known to have a link to a PEP (this includes any directors, beneficial owners, ultimate controllers, beneficiaries and agents as the case may be).

The identification of AML/CTF risks potentially faced by the Firm enables the Firm to design and implement the controls and measures required to mitigate and manage these risks.

Some risk themes currently faced by the Firm have been set out below (this list is not exhaustive):

- Live chat facility;
- The Firmˆs customer base is growing and from countries all over the globe;
- Interactions are non-face to face, a method preferred by criminals;
- Various electronic forms of payment credit cards used to trade;
- E-payments is a known method to dispose of illegally obtained funds, i.e. spending or receiving illegitimate money via trading accounts.

For the purposes of AML regulations, in identifying its AML/CTF risks, the Firm has considered the risks posed by the factors listed above and set out in detail below. These factors can result in a higher AML/CTF risk.

At a high-level, risk factors that the firm may reasonably face are identified as follows:

6.6.1 Customer Types

Including beneficial owners of customers,

- Any politically exposed persons PEP˚s (domestic and foreign);
- Customers who are identified as being persons or entities which support terrorist activity or are named in government lists or with credible sources in respect of corruption and/or criminal activity;
- The customer is not a resident in the UK and a foreign country with AML/CTF legislation comparable to the UK;
- Nature, volume and frequency of trading having regard to the financial standing of the customer;
- Customers (not necessarily PEPs) based in, or conducting business in or through, a high risk geographic location, or a geographic location with known higher levels of corruption or organised crime, or drug production/distribution;
- Opportunities are presented for criminals to engage in transnational activities have expanded with globalisation and advancements in information and communications technologies. Cyber-criminal activities increasingly affect the financial security of online business. It is widely accepted that the financial and insurance industry is the ˛target of choice˚ for financially motivated cyber criminals;
- Professional service providers such as lawyers, accountants, investment brokers or other professionals holding accounts for their customers or acting on behalf of their customer and where we would be required to place an unreasonable reliance on the professional service provider;
- Requests for undue levels of secrecy with a transaction;
- Whether the customer is a long-standing customer or undertakes occasional transactions;
- The customer˚s business activities place the customer in a high-risk category;
- Customers who wish to use pre-paid credit cards and the associated risks with the digital payments arena.

6.6.2 Business Relationships

With customers,

- Risks arising from changes in the nature of the business relationship, control structure or beneficial owner of the Firm˚s customers; and
- Intended type and level of transactions to be carried out and risks associated with those transactions. Larger transactions present higher AML/CTF risk.

6.6.3 Ownership Structures

- The Firm can only be satisfied that it knows who the beneficial owner is if they know who ultimately owns or controls the customer − either directly, or indirectly through interests in the customer˚s beneficial owner(s);
- Where there is a failure to identify who ultimately controls the business relationship preventing developing a clear understanding of the AML/TCF risk associated with the business relationship;
- Where the structure of the customer/entity renders it difficult to identify the true controlling

owner, or where there is no legitimate commercial rationale for the structure.

6.6.4 Delivery Methods

That is to say, methods by which we deliver financial services:

- Online
- Telephone (only if platform outage experienced)
- Live chat facility

6.6.5 Foreign Jurisdictions

Risks posed by foreign jurisdictions:

- Countries identified by credible sources (such as the Financial Action Task Force "FATF") as providing funding or support for terrorist activities or who have terrorist groups working within the country;
- Countries subject to sanctions, embargoes or similar measures;
- Countries identified by credible sources as having significant levels of corruption and/or criminal activity;
- Countries identified by credible sources as lacking appropriate AML/CTF legislation/ systems/ measures or controls;
- Countries identified by the FATF as non-co-operative countries and territories;
- Countries identified by credible sources as being tax havens;
- Countries that are materially associated with production and/or transnational-shipment of illicit drugs.

6.7 Client Risk Assessment

The Firm's client base is divided into three risk categories: Low, Neutral and High. The MLRO determines which category a client belongs. The MLRO will record the basis of assessment for each client.

Irrespective of the size and nature of the transactions or proposed transactions and exemptions, identity must be verified in all cases where money laundering or terrorist financing is known or suspected. If money laundering is known or suspected, then a report must be made to the FIU. Knowledge or suspicion of terrorist financing should be reported to the Commissioner of Police. In both cases, verification procedures must be undertaken if this has not already been done.

Where the MLRO has taken a decision to apply simplified CDD measures, the Firm must retain documentation that supports the basis for arriving at this decision.

The following should be used as guidance when applying a risk-based approach to the assessment of money laundering risk posed by each client. Consideration of the overall information held or gathered through the application process may alter the risk profile of the client.

6.8 Low-Risk

- Pension schemes;
- Occupational retirement/pension plans which do not allow non-employee participation;
- Financial institutions regulated by the Central Bank, the Securities Commission, the Office of the Registrar of Insurance Companies (the Registrar of Insurance"), or the Gaming Board;

- Regulated credit or financial institutions located in jurisdictions specified in the First Schedule of FTRA, FATF or Equivalent Jurisdictions, which is regulated by a body having equivalent regulatory and supervisory responsibilities as the Central Bank the Securities Commission, the Registrar of Insurance, or the Gaming Board (a list of Equivalent Jurisdictions and FATF Member Countries is included in an Appendix attached to this Manual).
- Government offices and agencies in all jurisdictions except for those in the Non-Cooperative Countries and Territories ("NCCTs") (a list of NCCTs is located at in the Appendix attached to this Manual);
- A publicly traded company or investment fund listed on The Bahamas International Stock Exchange or any other Stock Exchange specified in the Schedule to the FTRR and approved by the Securities Commission or equivalent exchange (a list of such exchanges can be found in an Appendix attached to this Manual).
- Domestic public authorities of countries of the European Economic Area.
- A regulated Investment Fund as defined in section 2 of the Investment Funds Act 2003 or regulated Investment Fund located in a country specified in the First Schedule of the FTRA and regulated by a body having equivalent regulatory and supervisory responsibilities as the Securities Commission; and,
- Any Bahamian dollar facility of or below $15,000.

6.9 High-Risk

- Relationships where a Politically Exposed Person ("PEP") or their connected person, have been identified as having a significant involvement.
- This definition of PEP would include heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned enterprises and important political party officials. Please consult the MLRO if you think that you may be dealing with PEP or their connected person. (See Chapter 6 of this Manual).
- Complex business ownership structures, such as offshore special purpose vehicles, that make it easier to conceal underlying beneficial owners, especially where there is no legitimate commercial rationale.
- Relationships involving clients that reside in or nationals of Non-Cooperative Countries and Territories ("NCCTs") (a list of NCCTs is located at in the Appendix attached to this Manual).
- Accounts that involve regular payments to or from unrelated third parties.
- Names that have been previously linked with financial crime (a Sanctions List can be found in the Appendix attached to this Manual).
- Clients based in or conducting business in or through high-risk jurisdictions with known level of corruption and organized crime, or drug production and distribution.
- Clients engaged in higher risk business activities (e.g. electronic gambling/gaming via the internet).
- Companies issuing bearer shares, especially if incorporated in higher risk jurisdictions.
- Clients that have been subject to a Suspicious Transaction Report.
- Clients that have not been physically present for identification purposes (i.e. non-face-to-face) (this does not apply to clients to whom SDD applies).

6.10 Neutral-Risk

All other clients that do not fall within either a low-risk category or a high-risk category including (but not restricted to):

- Subsidiaries of or entities associated with low-risk clients.

- Individuals residing from The Bahamas, the UK, EU or Equivalent jurisdictions.
- Private companies from The Bahamas, the UK, EEA or Equivalent jurisdiction provided they are not undertaking high-risk business.

6.11 Additional Considerations

The Firm will take the following additional considerations into account when determining the risk posed by a particular client. While these considerations will not determine the risk on their own, they will be considered alongside other factors in judging the overall money laundering risk posed by a particular client.

- Whether the Firm is engaged in a one-off transaction or business relationship.
- The nature and length of any existing or previous relationship between either Firm or our employees and the client.
- The way in which information is obtained (e.g. from a government department, regulated firm or other source).
- The nature and extent of any assurances given by other regulated firms that may be relied upon.
- Any associations the client may have with other entities or jurisdictions, such as headquarters, operating facilities, branches or subsidiaries and the individuals who may influence its operations.

Other relevant considerations; such as whether the client has a regulated investment manager or adviser, a prime broker (who have performed due diligence on the client) and other considerations that the MLRO may reasonably consider relevant to the client˚s risk assessment.

7. CLIENT ON-BOARDING

7.1 AML/CTF Policy Overview

- This AML/CTF policy is risk based.
- The Firm places focus on exercising judgment to reflect the risk-based nature of the legislation.
- The Firm identifies, verifies and then assesses the client.

The following steps are performed in identifying, verifying and performing a risk assessment of the customer:

7.1.1 Know Your Client (˜KYC˚) Information

Initial KYC information is obtained to identify and verify the customer as required by the money laundering regulations.

The Firm will initially seek to identify and then verify the customer is who they claim to be. As a result, initial questions and information must be obtained to identify (and verify) the person.

Beneficial owners and control structures are determined and CDD information is collected and verified. The Firm identifies major shareholders; understand the customer˚s management structure to determine control structures.

The Firm has outsources its CDD verification procedures to GB Group, a firm specializing in electronic checking and affirmation of identities. When a customer does not pass electronic

verification, then manual verification is under taken. Credit reporting agencies such as Experian is used for the manual verification process. FIRM does not utilize simplified due diligence methods.

7.1.2 Politically Exposed Persons (‘PEP’)

Identifying whether a customer is a PEP or on a sanction list is the next step of the client on-boarding procedure.

The Firm determines whether any customer or beneficial owner is a PEP (domestic, or foreign).

Where a customer is determined to be a PEP, the Firm collects and verifies KYC information and undertakes enhanced due diligence methods. The Firm then determine whether the PEP poses a AML/CTF risk. If classified high-risk, the application will not be accepted.

Compliance approval is required before providing a PEP with regulated services or establishing or establishing business relationship with them.

If a positive ‘hit’ is returned for one of the sanction lists, that applicant is not accepted.

7.1.3 Additional Due Diligence

Where the identity is unclear or non-verifiable, additional KYC information is obtained to identify and verify the customer.

If the minimum KYC information is considered insufficient and the Firm is unable to identify and verify the customer, then further (additional) questions are asked of the customer so that the identity of the customer can be verified with confidence.

7.1.4 Risk Assessment

A risk assessment is performed with respect to that customer prior to approving an account opening.

The risk assessment measures the firm’s exposure to facilitating money laundering and/or terrorism financing by its customer. The risk assessment is carried out in order to identify, mitigate and manage any AML/CTF risks.

To mitigate risk, the Firm has taken the decision that customers deemed to be high-risk at the outset are not approved or accepted.

8. ENHANCED DUE DILIGENCE (‘EDD’)

Although it is the Firm’s policy not to accept customers identified as high-risk at the outset, it has implemented an Enhanced Due Diligence (‘EDD’) program to include systems and controls to ensure, where appropriate,

- that the customer’s identity is established by additional documents, data or information;
- supplementary measures to verify or certify the documents supplied, or requiring confirmatory

certification by a credit or financial institution which is subject to money laundering regulations.

The Firm has implemented systems so that ongoing due diligence is conducted on the business relationship and scrutinising transactions to ensure that the transactions are consistent with the knowledge of the customer, and their business and risk profile.

8.1 EDD Criteria

Enhanced due diligence will be undertaken for all high-risk customers and transactions and where:

- there is a requirement to access further information in order to clarify & update KYC info;
- obtain further KYC info;
- there is consideration to investigate the suspicious transaction;
- verification or re-verification of information is needed;
- a more detailed analysis and monitoring transactions is required; and,
- there is a report of suspicious activity.

8.2 EDD Process

Where it is determined that enhanced due diligence should be applied, the process will be as follows:

- Compliance will conduct a thorough investigation to determine the source of the client˄s and each beneficial owner˄s wealth;
- Check the validity of the account registration details;
- Review any linked accounts;
- Re-verify KYC information;
- Analyse the customer˄s past transactions and possibly monitor future transactions if deemed necessary;
- Identify the purpose or nature of specific transactions;
- Check IP address where possible to detect any suspicious connection sources;
- Determine if any suspicious activity report should be lodged in accordance with procedures.

9. MONITORING

9.1 Introduction

Due to Firm˄s size and nature of its business, the Firm, in monitoring clients˄ activities, places reliance on two main factors:

1) Having up-to-date client information; and
2) Asking pertinent questions to elicit the reasons for unusual transactions

9.2 Methods

Ongoing monitoring of business relationships and client due diligence measures is an important component in mitigating and managing AML/CTF risks, both potential and identified. The Firm maintains an ongoing relationship with its clients through updating KYC information, transaction monitoring and by conducting enhanced customer due diligence. Monitoring takes place using a variety of methods.

Quarterly re-screening is conducted by the support team for existing PEPs and sanction matches. A sample of accounts are selected at random where the sample comprises of applications from higher risk countries.

The Firm has processes in place to determine when further KYC or beneficial owner information should be collected or verified to review and update information. All client records are reviewed and updated where the AML/CTF risk warrants this. This applies to both new and existing clients.

All new accounts are screened for errors by the new accounts team with supervision, guidance and account sign off from Compliance.

Sales and support staff maintain ongoing relationships and contact with clients. This contact is both for commercial purposes, to provide ongoing technical support and for the purposes of updating and maintaining KYC information by verifying name, date of birth and address. All notes are recorded in the firm˚s CRM database. Where appropriate, clients are requested to provide evidence in the form of proof of address documentation (such as a utility or bank statement) to action a change of address on the system.

Each member of the Firm˚s sales team maintains a list of client relationships, and the clients on the list are monitored daily. Contact is therefore maintained with all clients. Ongoing monitoring is undertaken during this process and KYC information verified to ensure it is up to date. Furthermore, if any suspicious activities are identified, a Suspicious Transaction Report (˜STR˚) procedure is initiated.

When a demo account is downloaded, a courtesy call is made by a member of the sales team. At this stage, the sales team member ascertains the trading experience of the customer. This enables the Firm to monitor and identify any unusual activities.

When withdrawal requests are received, client accounts are flagged for the attention of Compliance when there are any suspicious activities or requests for third-party transfers.

If any errors are identified within a client˚s account, or any suspicion is formed, account opening staff members contact the client.

The accounts and trading teams review transactions, including trading and electronic fund transfers, in the context of other account activity to determine patterns of any suspicious activities.

9.3 Up-To-Date Client Information

The Firm ensures that the information we keep about our clients is up-to-date through regularly performing client reviews. The frequency of such reviews is determined by the client˚s risk category. We review our clients with the following frequency:

- Low-risk clients are re-assessed every two years;
- Neutral-risk clients are re-assessed every year; and
- High-risk clients are re-assessed quarterly.

The purpose of these reviews is to identify any significant changes to the corporate structure, management and activities of the client. Unless the MLRO resolves otherwise, it is not always necessary to obtain all the information required for account opening or to re-verify all identification information. These reviews are coordinated by the MLRO. In addition to reviewing changes to the client˚s structure, management and profile an overall review of the client˚s activity over the period is

normally conducted. This will allow the Firm to assess if there have been changes in the client's activity which could be considered unusual given the information held about the client.

Notwithstanding these timescales, should any employee become aware of a change in the circumstances of a client, for example change of ownership structure or move into a new business area, this information should be recorded on the client file immediately. If this information could affect the risk assessment of the client, then the MLRO should be informed. The MLRO will then decide if there is the need to re-evaluate the client's risk assessment.

9.4 Transaction Monitoring

Due to the nature of its business the Firm relies on employees and the compliance monitoring program to monitor and identify suspicious transactions. The Firm considers that a combination of anti-money laundering training and commercial awareness will enable its employees to monitor, recognise and report suspicious activities.

In general terms, employees should have regard to the following considerations when monitoring client accounts, as well as other factors detailed in other chapters of this Manual:

- The unusual nature of a transaction: e.g., abnormal size or frequency for that client or type of client.
- The nature of a series of transactions: for example, a number of cash credits.
- The geographic destination or origin of a funding payment: for example, from a high-risk jurisdiction.

The Firm recognises that client behaviour may vary widely, therefore making it harder to pick up unusual or suspicious trading activity. Also, because the Firm does not provide advice to clients and does not own suitability obligations to them, we will hold little information about their trading motives.

When the Firm opens a client account on a non-face-to-face basis, and the payment is proposed to be made into an overseas account, the Firm will seek to mitigate this risk by establishing that the overseas account is held in the client's own name. If we are unable to establish this, we will review the account and transaction history; and enquire of the reason for making the payment abroad. This way we will seek to determine whether the account, or any dealings on it, are unusual, and therefore possibly suspicious.

The trading team monitors client trading activity, including electronic fund transfers on an ongoing basis. Staff are trained to identify 'triggers' requiring follow up due diligence. For example, disconnected telephone numbers or returned mail would trigger a client account's suspension until the KYC information is updated.

Staff are trained to identify and verify beneficial ownership information for all non-individual customer types on an ongoing basis. Where beneficial owner or true controllers are determined, additional KYC information is collected and verified.

On a case by case basis, the Firm monitors transactions of customers, including complex or unusually large transactions and odd patterns of transactions which have no apparent economic or visible lawful purpose.

On a case by case basis, staff on the account opening team manually monitor client accounts for suspicious activity.

Client accounts are monitored by staff on an ongoing basis in order to identify any suspicious activity. Staff review deposits and trading activity to ensure transactions comply with AML/CTF policies. Suspicious patterns trigger an escalation procedure and are reported to the team's line manager who will notify Compliance and an investigation will pursue.

If you have any doubts about the proposed transaction, you must report your suspicion to the MLRO. If the MLRO decides to make an external report to the FIU, they must obtain an appropriate consent, prior to making the overseas payment.

However, the Firm recognizes that while training is important, it is not a comprehensive substitute for transaction monitoring. Therefore, the Compliance Monitoring Program which is reported on a quarterly basis will seek to undertake specified tests to ensure that clients have been introduced in accordance with the Firm's policies and procedures.

9.5 Triggers and 'Red Flags'

Accounts and sales staff are trained to identify specific client activities that trigger red flags. There are a number of instances triggering a red flag including:

- The customer attempts to make frequent or large deposits of currency, insists on or asks for exemptions from the Firm's policies relating to the deposit of cash and cash equivalents.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force.
- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
- The customer's account indicates large or frequent wire transfers, immediately withdrawn without any apparent business purpose.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another Firm, without any apparent business purpose
- The customer makes a funds deposit for the purpose of pursuing a long-term trading strategy, followed shortly thereafter by a request to transfer the proceeds out of the account,

9.6 Record Keeping

Evidence of all monitoring undertaking by the Firm will be retained for a period of at least seven years from the date of the review.

10. SUSPICIOUS TRANSACTION REPORTING ('STR')

10.1 The Value of STRs

Suspicious Transactions Reports provides a critical intelligence gathering function, and can often present valuable opportunity for Law Enforcement to intervene in criminal activity. More values are listed below:

- STRs provide information and intelligence to law enforcement which is predominantly used in relation to financial crime and money laundering but can also be helpful in relation to other criminal activity.
- They provide information that assists in ongoing operations such as telephone numbers, addresses, alias identities, companies, investment activity, bank accounts and other assets. For example, information from STRs has assisted in kidnap cases and in locating a convicted escaped paedophile.
- STRs can help identify organised criminal schemes, for example mortgage and boiler room frauds, enabling detection and prevention activity including the issue of alerts to businesses at risk from such activity.
- Multiple STRs on the same subject or company can identify new targets for operational activity. Information leads to the recovery of the proceeds of crime by assisting in restraint orders, confiscation orders and cash seizures.
- STRs provide intelligence about criminal methods, contribute to law enforcement˚s understanding of crime and improve strategies to reduce the impact of crime.
- At a strategic level STRs data can inform policy and direct resources.
- STRs can help establish a geographical picture or pattern of the vulnerability of a particular sector or product, and can be used in the analysis of suspicious activity before and after a specific event (e.g. a terrorist incident).

10.2 Obligation to Report

Every employee, whether approved by the regulator or not, is required to make a formal report to the MLRO if, in the course of their employment, they know, suspect, or have reasonable grounds for either knowing or suspecting money laundering or terrorist financing. Any report submitted in accordance with this requirement will not result in the breach of any data protection laws, confidentiality or any other contractual or statutory provisions.

Remember that a duty to report a suspicion of money laundering exists even if a potential client does not conduct any business through the Firm, or if we decline the business. The obligation to report is in respect of anyone, whether the Firm˚s client or not.

10.2.1 Objective Test

It is important to understand that a person could be found guilty of a failure to report even if they did not actually suspect but ought to have suspected money laundering. The test is whether an honest and reasonable person, working within the financial services industry, would have formed a suspicion based on the facts available at the time. Generally, to satisfy this test you would have to know your client, their business and the rationale for their instruction, activity or transaction. A failure to make adequate enquiries or assess relevant facts will not provide protection against the objective test of reasonable suspicion.

10.2.2 Timing of Reporting

The obligation is to make a report as soon as reasonably practicable.

10.2.3 Discharge of Individual Responsibility

By submitting a report to the MLRO you will discharge your individual responsibility under POCA, thus protecting yourself from criminal prosecution for the offence of a failure to disclose. Therefore, when reporting a suspicion, you will receive a formal written acknowledgment from the MLRO. Please retain it for your own records.

10.2.4 Consultation with a Colleague or Line Manager

It is acceptable to discuss your suspicion with your immediate manager. However, if after consulting your immediate manager you remain suspicious, it is your responsibility to ensure that a report is submitted to the MLRO.

While your manager may comment on the proposed report, they do not have the authority to block or attempt to block any report being made to the MLRO. Should you encounter an attempt to prevent a report being made, you should discuss this with the MLRO directly.

In addition, if you consult a colleague, this colleague will have knowledge on the basis of which they must consider whether or not to make a report to the MLRO. To avoid making duplicate reports, the colleague, if suspicious, should only report if they are reasonably satisfied that the employee will not make such a report.

To reduce the risk of inadvertently tipping off a client, the case should be discussed with as few people as possible.

10.2.5 Continuous Obligation to Report

Making a report does not remove the need to notify the MLRO of further suspicions that may arise with the same or different client. If further suspicions arise additional reports must be made to the MLRO.

10.2.6 After Submission of a Report

Until the MLRO informs you that no report to the FIU is to be made, any further transactions or activity in respect of the suspected client must be reported to the MLRO as soon as they arise.

10.3 MLRO˙s Determination

The MLRO will consider the report and surrounding circumstances and decide whether or not to submit an external report to the FIU. If the MLRO decides to do so, they must do this as soon as practicable.

In order to undertake this investigation, the MLRO may need further information or access to client files. The MLRO must be given free access to all client records. If further information needs to be obtained from the client or from an intermediary, then this should normally be obtained by the employee with the client relationship. This is to minimise the risk of alerting the client or intermediary that a disclosure of the FIU is being considered.

The MLRO will record all internal enquiries made in relation to the report of a suspicion and the basis for their decision to make or not to make a report to the FIU.

A failure to make a report when there are reasonable grounds for a suspicion may constitute assistance under POCA.

If a disclosure to the MLRO causes them to acquire knowledge or suspicion of money laundering (or gives them reasonable grounds for such knowledge or suspicion) and the MLRO fails to make a report to the FIU, then they will be committing the offence of a failure to disclose under POCA.

10.3.1 Pre-Transaction Reporting to the FIU

If a pre-transaction report is made by the MLRO to the FIU, no business may be conducted with or for a client until you receive consent from the FIU. The FIU has 7 working days, from the working day following the day of the disclosure, in which to respond to the MLRO. Dealing with or advising a client before receiving consent from the FIU may constitute one of the offences under POCA, that is concealing, arrangements or acquisition, use and possession.

Note there are no provisions under the Act for consent to be given within a specified period. If a report is made to the FIU under this Act no related transaction or activity is allowed to proceed until the Firm has been contacted by the FIU or a law enforcement agency.

The MLRO will inform you whether the FIU consents to you dealing with the client or not. Please liaise directly with the MLRO who will provide guidance on what information may be provided to a client or potential client.

10.3.2 Post-Transaction Reporting to the FIU

Since the FIU cannot provide consent after a transaction or activity has already occurred, it will provide an acknowledgment of receipt of a report to the MLRO. In the absence of an indication to the contrary from the MLRO, you may deal with the client as normal. However, you must inform the MLRO of every interaction with the client and seek guidance on how to deal with that client.

10.4 Contact with Client and Third Parties

Any contact from the client questioning the delay in processing their transaction needs to be handled very carefully. In these circumstances please liaise closely with the MLRO.

Whether or not the FIU allows you to proceed with a transaction, you may not tip off the client that a disclosure to the authorities has been made. Neither may you disclose that such a disclosure has been made in response to a data protection request.

Unless specifically authorised to do so, you must not discuss any reports of suspicions of money laundering with third parties. Any requests for information from third parties, such as the Police or Customs, must be immediately referred to the MLRO.

10.5 Court Orders

Any evidence to be presented in Court will be obtained under a court order. The following are the types of order that may be served on the Firm as part of an investigation.

- Production order;
- Disclosure order;
- Client information order;
- Account monitoring order;
- Search and seize warrant; or
- Order for financial information under any of the Acts.

All such orders should be passed to the MLRO immediately who will liaise with Firm˚s legal advisers as appropriate.

10.6 Failure to Make a Report

In addition to the sanctions under the POCA and any one of the Acts, the Firm may take disciplinary action against any employee who fails to report a suspicion without a reasonable excuse.

10.7 Form of Reporting

Please make your report to the MLRO on the Suspicious Transaction Reporting Form (Money Laundering) attached as Appendix 1. Please give as much information on this form as possible to assist the MLRO.

10.8 Examples of Suspicious Activity

Below is a list of activities that may give rise to a suspicion of money laundering or terrorist financing. This is not an exhaustive list of circumstances; neither will they necessarily give rise to a suspicion. However, any of these occurrences is likely to form a basis for further enquiry in most cases. It will be ultimately a matter for your own consideration to decide whether or not to report a suspicion.

- Transactions with no apparent purpose or that make no economic sense;
- The client refuses to provide the information requested;
- Accounts that are used for a short period of time only;
- Dormant accounts that get reactivated;
- Extensive use of offshore structures, especially if they do not make economic sense; or
- Unnecessary routing of funds through third party accounts.

10.9 Relationships with Suspicious Clients

The Firm˚s policy is not to maintain relationships if the Firm believes that we may be used for money laundering. Where a client has been involved in a suspicious transaction, the MLRO, together with the senior management, makes a decision regarding the ongoing relationship with that client. If we decide to continue a client relationship, we may implement increased monitoring of the client˚s account. Where a client has been the subject of a referral to the FIU by the MLRO, the MLRO must be informed before any action is taken to exit the relationship. In such circumstances, the MLRO will consult the FIU to obtain permission to terminate the client relationship.

10.10 Record Keeping

Under the Acts it is an offence to destroy any documentation which may be relevant to a money laundering investigation. Records of all internal and external reports together with any supporting documentation must be retained for seven years from the date of the report. If, however, the firm is aware of an ongoing investigation in relation to any report it must be retained until the relevant agency has confirmed that the case is now closed.

11. ON-GOING RISK ASSESSMENT

Risk management is a continuous process. The MLRO is responsible for ensuring the Firm˚s risk assessment is up to date and appropriate. This is done by means of an on-going risk assessment.
On an on-going basis, the MLRO will review the Firm˚s business activities, including:

- Appropriate procedures to identify changes in client characteristics, which come to light in the normal course of business or at the account application process;
- Ways in which different products and services may be used for money laundering or terrorist financing, and how these ways may change;
- Adequacy of employee training and awareness;
- Monitoring compliance arrangements (such as internal audit/quality assurance, processes or external review);
- The balance between technology-based and people-based systems;
- Capturing appropriate management information;
- Upward reporting and accountability;
- Effectiveness of liaison with other parts of the Firm˚s Group; and
- Effectiveness of the liaison with regulatory and law enforcement agencies.

The MLRO will identify any changes to the Firm˚s services that may expose the Firm to a higher risk of money laundering. This may also highlight the need for a formal assessment of risks posed by either of our client categories or individual clients. The results of this on-going assessment will be detailed in the MLRO˚s Annual Report to senior management.

11.1 Annual Report

As part of its AML/CTF obligations under the laws and regulations, the Firm requires its MRLO to produce an annual report to ensure the Firm˚s systems and controls are proportionate to the size, nature and complexity of the operations and remain effective at all times.

The report includes an assessment and evaluation of:

- the adequacy of management information systems in place to deliver the information required by the senior management to ensure compliance with their responsibilities;
- the Firm˚s operation and effectiveness of its anti-money laundering systems and controls;
- appropriate coverage of new products and services, material changes in new customers take-on procedures, impact of new regulatory changes in business profile;
- the way in which new national and international findings have been used during the year.

The report shall also provide detail on:

- the number of reports made by staff to the MLRO, dealing separately, if appropriate, with different parts of the firm˚s business;
- documentation of risk management policies and risk profiles;
- monitoring arrangements to ensure that all areas adequately covered; and

The MLRO annual report is presented to the Firm˚s senior management where it is determined that arrangements be put in place to rectify any deficiencies identified. In particular, the report should satisfy senior management that the Firm˚s arrangements in regard to ensuring that suspicious activities are identified and reported to the MLRO are adequate, and also that they are satisfied that the effectiveness of the overall Identification and know your customer (KYC) procedures have been adequately managed and tested.

12. OVERSIGHT

The Firm's senior management is dedicated to overseeing the AML/CTF program and have ultimate responsibility for ensure compliance. Responsibility for ensuring policies and procedures are carried out in a manner to comply with AML/CTF laws and regulations is delegated to the firm's Chief Compliance Officer and Money Laundering Reporting Officer.

This AML/CTF policy has been adopted by the Board of Directors. Any amendment to this AML/CTF policy is subject to the Board's oversight and approval (i.e. the Board must formally adopt any amendment to the AML/CTF policy).

AML/CTF is a standing item on the Compliance Committee agenda. Compliance Committee Meetings take place on a monthly basis.

12.1 Appropriate Policies and Procedures

This AML/CTF policy has been designed to ensure and demonstrate compliance with AML/CTF obligations.

Money laundering and terrorist financing schemes can be difficult to identify and criminals can be ingenious in formulating different schemes to facilitate their money laundering or terrorist financing agendas.

Accordingly, for this policy to be effective, it requires regular review and if necessary, amendment, in order that it accomplishes its purpose of identifying, mitigating and managing AML/CTF risk.

Compliance is notified and acceptance is sought prior to the Firm:

- Introducing a new designated service to the market;
- Introducing new methods of delivery of a regulated service; and/or;
- Introducing any new or developing technology used for the provision of financial services.

This will enable Compliance to identify any significant changes in AML/CTF risks and to formulate controls to mitigate and manage those risks.

12.2 Client Identification Procedures

(Commonly known as 'Know your Customer/Client' or 'Due Diligence' procedures)

KYC procedures are risk based having regard to the AML/CTF risks relevant to the provision of the services offered. The procedures are designed to mitigate and manage the potential AML/CTF risks and ensure that the firm is reasonably satisfied as to the true identity of its clients.

12.3 Training

Appropriate training with regard to money laundering and terrorist financing is vital in managing the AML/CTF risk. Accordingly, all staff are required to undergo regular training in AML/CTF laws, regulations and internal policies.

All employees of the Firm are (1) made aware of the law relating to money laundering and terrorist financing; and (2) given training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.

Training is carried out under the supervision of compliance and senior management. Ongoing general refresher training for all staff will occur on an annual basis. AML/CTF closed jurisdiction list updates are circulated to all staff monthly. In-house AML/CTF awareness training and assessment is compulsory for all staff.

Training is developed and provided in-house. Delivery of the training includes written updates, educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos.

Records of training are maintained recording staff attendance, the dates of training, and a brief description of the subject matter provided.

All employees are provided with a copy of the Firm's AML/CTF policy and are required to confirm awareness and understanding obligations on an annual basis.

13. TRAINING AND AWARENESS

13.1 Introduction

For the purpose of this manual 'awareness' refers to actions taken by the Firm to ensure that on an ongoing basis personnel are informed of money laundering and associated risks as well as their individual and collective responsibilities.
'Training' refers to a more specific process whereby employees are educated on specific areas, their attendance is recorded and understanding measured normally by way of a short test or a question and answer session.

The Firm has a legal responsibility to ensure that personnel receive appropriate anti-money laundering training. Failure to provide training may constitute a criminal offence.

13.2 Awareness

It is our policy to ensure that all employees are aware and kept up to date with money laundering developments. This Manual serves as the basis for awareness within the Firm. It will be supplemented with additional material as and when necessary.

At the start of their employment every employee must be given a copy of this Manual and must sign an Anti-Money Laundering Manual Declaration attached as Appendix 7 to confirm that they have read and understood the provisions of this Manual.

13.3 Training

The Firm provides training to relevant employees upon recruitment and thereafter on an annual basis. The definition of 'relevant employee' is set as widely as possible to encompass all employees who may be able to identify suspicious transactions during the course of their work. The requirement to train a relevant employee is also applicable to any part-time, temporary or consulting employee.

Anti-money laundering training will, as a minimum, comprise the following issues:

- The need to obtain sufficient evidence of identity;
- Recognition and reporting of suspicions of money laundering via the MLRO to the FIU;
- The identity and responsibilities of the MLRO;
- Anti-money laundering rules, guidance and regulations; and,
- Effects of breaches of money laundering legislation on the Firm and its employees.

The attendance or completion of anti-money laundering training is mandatory for all relevant personnel. If you are unable to attend on a scheduled training date you should contact the course organiser or provider as soon as possible to arrange an alternative date. Repeated failures to attend training courses may result in disciplinary action.

If, after attending a training course, you feel that you would benefit from further clarification on certain subjects, please contact the MLRO.

13.4 Record Keeping

The Firm will retain the records of all materials issued to its personnel in relation to anti money laundering training and awareness for at least seven (7) years from the date of issue of materials. These records will include the attendee registers, dates of all training sessions, content of courses and presentations and, where applicable, tests results.

14. RECORD RETENTION

14.1 Introduction

This chapter provides guidance on the record keeping procedures that the Firm needs to meet their obligations in respect of the prevention of money laundering and terrorist financing.

Keeping adequate records will ensure that the Firm can:

- Provide an audit trail for all advice given and activity undertaken on a client˙s behalf;
- Provide adequate information to the law enforcement agencies to assist with their investigations;
- Undertake monitoring of client activity against expectations;
- Identify and report any suspicious activity; and,
- Provide evidence of meeting all statutory and regulatory obligations.

14.2 What records have to be kept?

The following material must be kept:

- Client information, including evidence of identify;
- Details of all transactions made on behalf of each client;
- Internal and external reports of suspicion;
- MLRO annual report and any other reports;
- Information not acted upon;
- Training and compliance monitoring; and,
- Information about the effectiveness of training.

Keeping the required records for the specified time period will not result in the Firm breaching any data protection laws. This information will be made available to the competent authorities in the context of any relevant criminal investigations and prosecutions.

14.3 Identification Records

Client identification records must be kept for a period of at least seven (7) years from the date of the end of a client relationship. That is either the date of the last transaction with the client or the closure of client account, whichever is the latest.

14.4 Transaction Records

Transaction records must be kept for a period of at least seven (7) years from the date of the transaction. They should be maintained in a form which provides satisfactory audit trail of all transactions effected via the Firm allowing their reconstruction.

14.5 Third party Record Keeping

If the Firm has an appointed representative, then it is the Firm˙s responsibility to ensure the representative complies with the record keeping obligations. This principle also applies to the use of third party service providers such as introducers or administrators.

14.6 Internal and External Suspicious Transaction Reports

The Firm will retain the following records of any reports of suspicions of money laundering regardless of whether the MLRO made a report to the FIU. These records will consist of:

- Records of actions taken under the internal and external reporting requirements;
- When the MLRO had reviewed an internal report and decided not to make a report to the FIU, a record of all the information considered; and
- Copies of reports of suspicions submitted to the FIU.

These records will be retained for seven (7) years from the date the report is made. However, if the Firm is aware that either the FIU or another law enforcement agency is conducting an investigation into a client, the Firm will retain all records in relation to that client until the agency confirms that the case is closed. If, within seven (7) years of a disclosure being made, the Firm has not been advised of an ongoing investigation, it may destroy the records.

14.7 Anti-Money Laundering Training Records

We will retain the following records for at least seven (7) years in relation to Anti-Money Laundering (˙AML˚) training:

- Date(s) AML training was given;
- Nature and content of the training;
- Names of people who received the training; and
- The results of the tests taken, if applicable.

14.8 Compliance Monitoring Records

The following records are retained for at least seven (7) years in relation to compliance monitoring:

- Annual MLRO report to the board and any other reports to senior management; and,
- Records of consideration of those reports and of any action taken as a consequence.

14.9 Refused Business Records

Where business has been refused because it does not meet our client identification, verification and KYC standards, a record of the refusal will be retained for seven (7) years.

14.10 Wire Transfer and Electronic Payment Records

All electronic payment messages should contain sufficient information to identify the parties involved (i.e. both the party making the payment and the beneficiary). This information should include full names, addresses and account numbers. Where this information cannot be provided in the electronic payment message, full records must be retained.

14.11 Format and Retrieval of Records

The Firm aims to reduce the volume and density of records. While still complying with the statutory requirements we may choose to keep records:

- By way of original documents;
- By way of photocopies of original documents; On microfiche;
- In scanned form; or
- In computerized or electronic form.

The Firm may keep records either offsite or outside the country, but will remain responsible for ensuring that all required records can be made available without undue delay and meet the regulatory requirements. The Firm will ensure that all records, however kept, are capable of being retrieved within 48 hours. The Firm will, whenever possible, seek to retain all records on the business premises.

14.12 Sanctions and Penalties

Where a firm fails to observe, the record keeping requirements either the Firm, or relevant person(s) or both are open to prosecution. This may include imprisonment, an unlimited fine and/or regulatory censure.

Name of Person Reporting a Suspicion:
Job Title or Responsibility:
Client˙s Name & Address:
Details of Event(s) Giving Rise to a Suspicion (use a separate sheet of paper if necessary):
Details of Supporting Evidence Attached (if any):
Is this report being made pre or post transaction?

Signature:

Date:

Please give this completed form to the MLRO or Deputy MLRO immediately, and retain a copy of this report for your own records.

To be completed by the MLRO
Client name:
Date received:
Date review completed:
Comments Regarding the Suspicion:
Reported to the FIU?

Yes copy of the FIU report attached.

If disclosure is prior to an event, have the appropriate measures been taken to ensure the transaction cannot proceed for the next 7 working days?

No basis for non-disclosure is included in comments above

Signature:

Date:

APPENDIX 2: AML/CTF COURSE REGISTER OF ATTENDEES

Date:

Course: ANTI MONEY LAUNDERING & COUNTER TERRORIST FINANCING TRAINING

With your signature below:
1) You confirm attendance in the training course; and,
2) You have understood the content covered.

Name	Signature

Please keep this register on file with a copy of the presentation and course materials.

APPENDIX 3: PROOF DOCUMENTS FOR NATURAL PERSONS

This is a non-exhaustive list of documents that may be acceptable when identifying a natural person if the Firm is unable to verify an individual's identity electronically:

Government-issued documents with a photograph include, but are not restricted to:

- Valid passport
- Valid photocard driving licence (full or provisional)
- National Identity card
- Voter's card

Other documents include, but are not restricted to:

- Current bank statements, or credit/debit card statements, issued by a regulated financial sector firm in The Bahamas, the UK, EU or Equivalent jurisdiction (but not ones printed off the internet)
- Utility bills
- Instrument of a court appointment (such as liquidator, or grant of probate)
- Current council tax letter, or statement

APPENDIX 4: USEFUL INFORMATION SOURCES

Financial Intelligence Unit (the FIU)
http://www.bahamas.gov.bs/FIU

List of Regulators
https://en.wikipedia.org/wiki/List_of_financial_regulatory_authorities_by_country

Sanctions List
https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets

Worldwide Registries (Companies House equivalents)
https://www.gov.uk/government/publications/overseas-registries

Equivalent Jurisdictions
www.jmlsg.org.uk/download/8201

Financial Action Task Force
The inter-governmental body known as the "Financial Action Task Force" ("FAFT") was established to develop and promote policies, both at national and international levels on combating money laundering and terrorist financing. FATF member countries have committed themselves to implementing the FATF Forty Recommendations which in several respects are more wide-ranging in nature than the provisions of the European Money Laundering Directives. Membership of this inter-governmental body is subject to ongoing approval and monitoring.
http://www.fatf-gafi.org/

FATF Member Countries
http://www.fatf-gafi.org/countries/#FATF

Non-Cooperative Countries and Territories (NCCTs)
The current list of countries and territories that are not cooperative in the international fight against money laundering can be found on the following website.
http://www.fatf-gafi.org/countries/#high-risk

Recognised Exchanges
Recognised Investment Exchanges, Recognised Overseas Investment Exchanges, Recognised Clearing Houses, Recognised Overseas Clearing Houses, Designated Investment Exchanges and Regulated Markets.
https://www.handbook.fca.org.uk/handbook/REC.pdf

APPENDIX 5: CURRENT LIST OF GLOBAL SANCTIONS AND ENFORCEMENT AGENCY DATA SOURCES

The current list of global sanctions and enforcement agency data sources available to FIRM to screen potential clients or applicants at the application stages and periodically:

Sanctions

- Bank of England
- Commission de Surveillance du Secteur Financier, Luxembourg
- De Nederlandsche Bank, Netherlands
- Department of Foreign Affairs and Trade, Australia
- European Union
- Financial Services Agency
- Guernsey Financial Services Commission
- Home Office, UK
- Hong Kong Monetary Authority
- Isle of Man Financial Supervision Commission
- Jersey Financial Services Commission
- Ministry of Finance, Japan
- Monetary Authority of Singapore
- Office of Foreign Assets Control (OFAC), US
- Office of the Superintendent of Financial Institutions, Canada
- Reserve Bank of Australia
- United Nations Security Council Committee
- US Department of State

Law Enforcement

- Central Bureau of Investigation, India
- Central Narcotics Bureau, Singapore
- City of London Police, UK
- Federal Bureau of Investigation (FBI), US
- General Police Directorate, Slovenia
- Hong Kong Police Force
- Interpol
- Metropolitan Police Force, UK
- Ministry of the Interior, Saudi Arabia
- National Crime Squad, UK
- Philippines National Police
- Royal Malaysian Police
- South African Police Service
- US Air Force of Special Investigations
- US Bureau of Alcohol, Tobacco, Firearms and Explosives
- US Drug Enforcement Administration
- US Immigration and Customs Enforcement

- US Marshals Service
- US Naval Criminal Investigative Service
- US Postal Inspection Service
- US Rewards for Justice
- US Secret Police

Regulatory Enforcement Bodies (UK)
- Assets Recovery Agency
- Financial Services Authority
- Gibraltar Financial Services Commission
- Guernsey Financial Services Commission
- Investment Management Regulatory Organisation
- Isle of Man Financial Services Commission
- Jersey Financial Services Commission
- Lloyds Insurance Market
- Personal Investment Authority
- Securities and Futures Authority

Europe (excluding UK) Enforcement Bodies
- Autorite des Marches Finance, France
- BaFIn, Germany
- Banking, Finance and Insurance Commission, Belgium
- Banque de France, France
- Capital Market Commission, Greece
- Comision nacional del Mercado de Valores, Spain
- Commission de Surveillance du Secteur Financier, Luxembourg
- Commissione Nazionale per le Societa e la Borsa, Italy
- Cyprus Securities and Exchange Commission
- Czech National Bank
- Danish Financial Supervisory Authority
- Financial Market Authority, Austria
- Financial Market Authority, Slovakia
- Financial Regulator, Ireland
- Financial Supervisory Authority of Norway
- Finnish Supervision Authority
- Hungarian Financial Supervision Authority
- Insurance Supervisory Commission of the Republic of Lithuania
- Malta Financial Services Authority
- Netherlands Authority for the Financial Markets
- Polish Securities and Exchange Commission
- Portuguese Securities Market Commission
- Securities Commission of the Republic of Lithuania
- Securities Market Agency, Slovenia
- Swedish Financial Supervisory Authority

- Swiss Federal Banking Commission

North American Enforcement Bodies

- Autorite des Marches Financiers, Canada
- British Columbia Securities Commission, Canada
- Commodity Futures and Trading Commission (CFTC), US
- Federal Insurance Deposit Corporation, US
- Federal Reserve Board, US
- Federal Trade Commission, US
- Financial Crimes Enforcement Network, US
- Financial Industry Regulatory Authority (FINRA), US
- Investment Dealers Association of Canada
- Manitoba Securities Commission, Canada
- Market Regulation Services Inc, Canada
- Mutual Fund Dealers Association of Canada
- National Credit Union Administration, US
- National Futures Association (NFA), US
- New York Stock Exchange, US
- Office of Foreign Assets Control (OFAC), US
- Office of the Comptroller of the Currency, US
- Office of the Superintendant of Financial Institutions, Canada
- Office of Thrift Supervision, US
- Ontario Securities Commission, Canada
- Saskatchewan Financial Services Commission, Canada
- Securities and Exchange Commission, US
- Securities Commission of Newfoundland and Labrador, Canada
- United States Court of International Trade, US

Latin American/Caribbean Enforcement Bodies

- British Virgin Islands Financial Services Commission
- Cayman Islands Monetary Authority
- Central Bank of Belize
- Central Bank of Bahamas
- Chilean Securities and Insurance Supervisor
- Comision Nacional Supervisora de Empresas Y Valores, Peru
- International Financial Services Commission, Belize

African/Asian/Pacific Enforcement Bodies

- Australian Prudential Regulation Authority
- Australian Securities & Investments Commission
- Central Bureau of Investigation, India
- Financial Services Agency, Japan
- Financial Services Board, South Africa
- Financial Services Commission, Mauritius
- Hong Kong Monetary Authority

- Hong Kong Securities and Futures Exchange
- Indonesian Capital Market Executive Agency
- InvesteED, Hong Kong SFC
- Monetary Authority of Macao
- Monetary Authority of Singapore
- Reserve Bank of India
- Securities and Exchange Commission Pakistan
- Securities and Exchange Commission, Republic of Philippines
- Securities and Exchange Commission, Thailand
- Securities and Exchange Surveillance Commission, Japan
- Securities Commission of New Zealand
- Securities Commission of Malaysia

Other Bodies

- Bureau of Industry and Security, US
- Centro Mexicano Para La Filantropia, Mexico
- Companies House, UK
- Financial Action Task Force (FATF)
- Ministry of Economy Trade and Industry, Japan
- World Bank

APPENDIX 6: SUMMARY OF EXISTING LAWS

A summary of Acts, laws and guidelines is contained within the AML/CFT Guidelines issued by The Bahamas' authorities.

http://www.centralbankbahamas.com/legal_guidelines.php?cmd=view&id=16620

It includes:

- the Proceeds of Crime Act, 2018 ("POCA") (as amended);
- the Anti-Terrorism Act, 2018 (as amended);
- the Financial Transactions Reporting Act, 2018 (as amended) ("FTRA");
- the Financial Transactions Reporting Regulations, 2018 (as amended) ("FTRR");
- the Financial Transactions Reporting (Wire Transfers) Regulations, 2009;
- the Financial Intelligence Unit Act, 2000 (as amended) ("FIUA");
- the Financial Intelligence (Transactions Reporting) Regulations, 2001 (as amended);
- the Securities Industry Act, 2011 (as amended) ("SIA"); and,
- the Securities Industry (Anti Money Laundering and Countering the Financing of Terrorism) Rules, 2015 (as amended) ("SIR")

APPENDIX 7: ANTI-MONEY LAUNDERING MANUAL DECLARATION

1) I hereby acknowledge that I have read and understood the provisions of the Firm's Anti- Money Laundering Manual ("Manual").
2) I agree to comply with the policies and procedures of the Manual. If I am ever unsure about any of the areas covered in this Manual I will consult the Firm's Money Laundering Reporting Officer.
3) I understand that a breach of any of the provisions of the Manual may result in criminal prosecution, regulatory censure or disciplinary action by the Firm.

Name:

Signature:

Date: