AML & CFT Programme

Contents

1. WHAT IS MONEY LAUNDERING?

1.1 Definition

Money laundering is a process of concealing the true origin and ownership of illegally obtained money. Principally, it is proceeds of criminal activities such as illicit drugs, corruption, organized crime, fraud, sex trade, forgery, illegal logging/fishing, revenue evasion, counterfeit money, piracy, terrorism etc., which criminals attempt to disguise.

1.2 Money laundering process

There is more than one method of laundering money. Methods can range from purchase and resale of real estate or a luxury item to passing money through a complex web of legitimate businesses and 'shell' companies. In most cases, the proceeds of these criminal activities take the form of cash. There are three stages of money laundering, during which there may be numerous transactions made by launderers that could alert us.

1.3 Placement

Placement is the physical disposal of the cash or asset derived from illegal activity. It includes the opening of numerous bank accounts, depositing cash, exporting cash, and using cash to purchase high value goods such as property or businesses.

1.4 Layering

Layering is the separation of criminal proceeds from their source by creating complex layering process of financial transactions designed to defeat the audit trail and provide anonymity. It may include telegraphically transferring funds overseas, depositing cash overseas, reselling goods previously with cash.

1.5 Integration

Integration provides apparent legitimacy to criminally derived wealth. If the layering process succeeds, integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds. This may be achieved through a complex web of transfers or income from apparently legitimate businesses previously purchased with the proceeds of illegal activities.

2. WHAT IS FINANCING OF TERRORISM?

Terrorist financing involves collecting and providing funds for terrorist activity. The primary objective of terrorism is 'to intimidate a population, or to compel a Government or an international organization to door abstain from doing any act'. The goal of the terrorist or terrorist organization is to maintain financial support in order to achieve their aims, and a successful terrorist group, is one that is able to build and maintain an effective financial infrastructure.

Terrorist needs finance for a wide variety of purpose – recruitment, training, travel, materials and setting up safe havens.

Terrorist control funds from a variety of sources around the world and employ sophisticated techniques to move funds between jurisdictions. In order not to be detected, a terrorist group

draws in the service of banks and nonbanking institutions and takes advantage of their services products.

2.1 Financing Terrorism and Associated activities

Terrorist financing is a financial crime that uses funds to support the agenda, activities or cause of a terrorist organization. The funds raised may be from legitimate sources, such as charitable organizations or donations from supporters, as well as criminal sources, such as the drug trade, weapons smuggling, fraud, kidnapping and extortion for illegal activities.

According to the U.S. State Department's "Country Reports on Terrorism (2013)," the most common method of terrorist financing is kidnapping for ransom. Other major sources include private donations, directly or indirectly through charitable organizations, revenue from legitimate businesses and illicit revenue from criminal activities (e.g., smuggling, narcotics trafficking).

2.2 Is the financing of weapons of mass destruction considered terrorist financing?

If the proliferator is a terrorist, financing weapons of mass destruction (WMDs) could be considered a type of terrorist financing. However, not all proliferators are terrorists; therefore the development of measures to prevent, suppress and disrupt the proliferation and financing of WMDs, distinct from terrorist financing, is necessary.

2.3 Are the stages of terrorist financing the same as money laundering?

In general, yes, however, in the placement phase, funds could be derived from both legitimate and illegal activities.

The methods of layering to disguise the source of funds are the same with money laundering and terrorist financing.

In the integration phase, funds are typically disbursed to the terrorist or terrorist organization, directly or indirectly through a third party to obscure the beneficiary and the ultimate objective of supporting a terrorist act.

2.4 If the predicate crime occurs outside of the United States, can one be charged with money laundering?

In many circumstances, dual criminality, where the illicit activity is considered a predicate offense to money laundering in both countries (e.g., crime occurred in one country, proceeds from the crime detected in another country), may be required to facilitate mutual legal assistance and, ultimately, prosecution for money laundering.

With the globalization of the world economy, the rise of transnational organized crimes and the focus on foreign corruption, mechanisms to coordinate international cooperation (e.g., information sharing, extradition, asset recovery) to combat money laundering and terrorist financing are more imperative than ever.

2.5 Have international standards been developed to combat money laundering and terrorist financing?

Yes. In 1990, FATF published 40 legislative and regulatory recommendations for combating money laundering and terrorist financing. These standards, published as the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – the FATF Recommendations and referred to as "FATF Recommendations" or "Recommendations" were revised in 1996, 2001, 2003 and 2012 In 2001, eight special Recommendations were added

to address terrorist financing. The Recommendations cover the following:

- AML&CFT Policies and Coordination (Recommendations 1 and 2) – Provides guidance on how to assess risks and apply a risk-based approach in developing an AML&CFT framework and how parties (e.g., financial institutions, regulatory authorities, law enforcement) can share information and coordinate efforts with each other, domestically and internationally.
- Money Laundering and Confiscation (Recommendations 3 and 4) – Advises countries to criminalize money laundering and apply it to the widest range of predicate offenses, and provides guidance on legislative measures to enable authorities to freeze, seize or confiscate proceeds and property from money laundering and terrorist financing.
- Terrorist Financing and Financing of Proliferation (Recommendations 5 – 8) – Advises countries to criminalize terrorist financing and designate terrorist financing as a money laundering predicate offense; provides guidance on the legislative measures to designate and delist targets and to enable authorities to freeze funds or assets of designated targets subject to sanctions related to terrorism, terrorist financing and proliferation of WMDs; encourages countries to review laws and regulations that relate to nonprofit organizations to evaluate their adequacy in guarding against abuse for the financing of terrorism.
- Preventive Measures (Recommendations 9 – 23) – Advises countries to modify secrecy laws to enable implementation of FATF's Recommendations (e.g., to facilitate information sharing between appropriate authorities); and outlines several measures or controls for financial institutions to mitigate risks and prevent money laundering and terrorist financing, including:
    - Risk assessments to identify vulnerabilities and appropriate controls to mitigate the risks associated with new customers, products and business practices, including new delivery mechanisms;
    - Development of an enterprise wide program, including policies on information sharing, consistently applied across foreign branches and subsidiaries, with enhanced measures for those located in high-risk jurisdictions;
    - Risk-based due diligence (e.g., collection of information at account opening and ongoing, verification of identity, reporting of suspicious transactions, obtaining senior management approval) on customers and beneficial owners, with enhanced measures for politically exposed persons (PEPs), correspondent banks, and money or value transfer services, also known as money services businesses (MSBs);
    - Ability to stop (e.g., freeze, seize, confiscate) transaction(s)/asset(s) if it involves a designated target subject to sanctions;
    - Reporting of suspicious transactions to financial intelligence units (FIU), with measures to ensure confidentiality and to protect financial institutions from criminal and civil liability (i.e., Safe Harbor);
    - Recordkeeping to permit reconstruction of transaction(s) and, if necessary, to provide evidence for prosecution of criminal activity, including, but not limited to, originator/beneficiary information in wire transfers;
    - Development of policies that outline the conditions under which a financial institution may rely upon a third party to perform due diligence on its behalf; and
    - Due diligence requirements for designated nonfinancial businesses and professions (DNFBPs) (e.g., casinos, real estate agents, dealers in precious metals and stones, attorneys, accountants, trust service providers).
- **Transparency and Beneficial Ownership of Legal Persons and Arrangements**

(Recommendations 24 –25) – Provides guidance on measures to prevent the misuse of legal persons or legal arrangements (e.g., trusts) for money laundering and terrorist financing, including bearer shares or bearer share warrants, by facilitating the collection of and access to beneficial ownership and control information.

- Powers and Responsibilities of Competent Authorities and Other Institutional Measures (Recommendations 26 –35) – Provides guidance on the development of an effective AML&CFT system, including, but not limited to:
  - Designation of competent and empowered authorities to supervise financial institutions and DNFBPs for compliance with AML&CFT laws and regulations with a risk-based approach
  - Establishment of an FIU as the central agency to receive and analyze required reporting (e.g., suspicious transaction reporting, large currency transactions, disclosures of cross-border movement of currency and negotiable instruments) and disseminate guidance, statistics and feedback to relevant authorities in a secure and confidential process
  - Designation of competent and empowered law enforcement authorities with the responsibility of conducting domestic and international money laundering and terrorist financing investigations, and the authority to identify, trace and initiate freezing and seizing of assets
  - Establishment of a large currency transaction reporting requirement above a fixed amount, including both domestic and international transfers
  - Establishment of a declaration or disclosure system to detect cross-border transportation of currency and bearer negotiable instruments (BNI), also referred to as monetary instruments
  - Establishment of sanctions (e.g., civil, criminal, administrative penalties) for noncompliance with AML&CFT laws and regulations for financial institutions, DNFBPs and senior management
- **International Cooperation (Recommendations 36 – 40)** – Countries are encouraged to ratify international conventions/treaties and develop a legal basis (e.g., sign treaties, enter a memorandum of understanding [MOU]) to provide mutual legal assistance (e.g., information sharing, freezing of assets, extraditions) to other countries (e.g., financial institutions, FIUs, supervisors, law enforcement) in relation to money laundering and terrorist financing proceedings. Suggested treaties include:
  - United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention, 1988);
  - United Nations Convention Against Transnational Organized Crime (Palermo Convention, 2000);
  - The United Nations Convention Against Corruption (2003);
  - The International Convention for the Suppression of the Financing of Terrorism (the Terrorist Financing Convention, 1999); and
  - Other relevant treaties where applicable.

3. OUR POLICY

3.1 Duty of Vigilance

We are expected by the AML & CTF Act and the FATF Recommendations to have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the institution from being used, intentionally or unintentionally, by money launderers and terrorism financiers.

The policies and procedures in this manual implement the duty of vigilance expected of us to avoid assisting the process of laundering and terrorism financing and to react to possible attempts at being used for those purposes.

3.2 Principles

- We oppose the crimes of money laundering and terrorism financing and do not tolerate the use of our products and services for either of these purposes.
- We are committed to playing our role in the fight against money laundering and terrorism financing.
- We will comply with the letter and the spirit of the laws and regulations that relate to AML & CTF.
- We will provide our products and services only for legitimate purposes to persons whose identities we have been able to reasonably ascertain.
- We will avoid relationships with those that we reasonably assess as representing too high a risk of money laundering or terrorism financing.
- We will help our staff manage the issues that might arise for them when dealing with people they know, including kin.
- Our owners, management and staff will be treated in the same way as all other Applicants when they apply to use our services.
- We report any activity that we detect which we regard as suspicious.
- Our staff will receive the AML & CTF training they need to understand their obligations under the law and to perform in their roles.
- We will monitor our customers, their transactions, and our people, consistent with the level of money laundering and terrorism financing risk they represent.
- We will comply with the requirement under the AML & CTF Act to register and inform them of any material changes that may occur within our business at any time.
- Our office will adhere to the requirements under the AML & CTF Act to report on the appointment of or update on any changes regarding our Compliance Officer.
- We are aware that our owners, management and staff are subject to a fit and proper screening and could be removed pursuant as a disqualified person within the meaning of the AML & CTF Act.

3.3 Our AML & CTF Program

Our AML & CTF Program is made up of the contents of this manual. Our activities can be described as a series of controls to manage the way we:

- accept applications for transactions;
- monitor the transactions we do for unusual activity that needs further investigation;
- identify events that require us to take further action;
- report certain matters;

- and Keep records of what we do.

Some of the controls we use are embedded in the way our products operate.

3.4 Disciplinary action and dismissal

3.4.1 Our staff will face disciplinary action, and possibly dismissal, if they fail to follow the AML & CTF procedures and requirements in this manual. We will dismiss any person who is involved in facilitating money laundering, terrorism financing or who launders money or finances terrorism using our products and services, and we will comply with any law that requires us to report such matters, including to law enforcement. Law enforcement receives our full cooperation in the prosecution of such matters against our staff.

3.4.2 Sometimes customers or transactions involve people we know well, or may involve the owners of this business or someone else close to us. Even if this is the case all our staffs are still expected to follow the procedures in this manual.

3.4.3 Staff should go to the Compliance Officer if they are experiencing difficulties with this area.

4. ROLES AND RESPONSIBILITIES

4.1 Purpose

It is essential that everyone in our organization understands what they have to do to comply with the requirements of this manual.

4.2 All staff and owners

- Are expected to comply fully with all of the procedures in this manual.
- Must receive regular AML & CTF training, including training about detection and reporting of unusual and suspicious activity by customers.
- Are expected to report any unusual or suspicious activity detected to the CO.
- Are expected to understand the law regarding tipping-off and comply with our anti-tipping-off procedures.
- Are expected to cooperate fully in the investigation of any possible breaches of the laws and regulations that relate to AML & CTF.

4.3 Owners

- Our owners set the tone for our business regarding its commitment to AML & CTF.
- Our owners must ensure that this manual meets the requirements of the laws and regulations that relate to AML & CTF and must oversee and monitor compliance with this manual.

4.4 Compliance Officer (CO)

The CO is a senior staff member is responsible for:

- Creating and keeping this manual current;
- Monitoring the compliance by our business with the requirements of the laws and regulations that relate to AML & CTF;
- Monitoring transactions undertaken for Customers;
- Identification and management of money laundering risk using our services;

- Providing leadership and training on AML & CTF issues to our staff, including new staff;
- Acting as the liaison point;
- Investigating unusual matters and reporting those that are suspicious;
- Reporting all other matters that must be reported;
- Ensuring that our staff know what their responsibilities are;
- Monitoring employees in the course of performance of their duties;
- Ensuring that our staff are aware of the requirements of this manual and of the AML & CTF laws and regulations that apply to our business;
- Helping our staff where they face problems associated with Customers who they know well or who are kind;
- Overseeing corrective actions where gaps are identified in our operations with the procedures in this manual;
- Reviewing this manual periodically for its adequacy;
- Arranging for periodic independent review of this man

4.5 Supervisors

Our supervisors are the most senior person on duty during our hours of operation and they are responsible for:

- Following the processes and procedures in this manual and being seen by the other staff to follow them;
- Ensuring that the staff they supervise follow the processes and procedures in this manual;
- Promoting required AML & CTF behavior by coaching, teaching, leading and encouraging other staff.
- Helping our staff where they face problems associated with Customers who they know well or who are kind;
- Allowing staff to attend AML & CTF training and awareness sessions;
- Cooperating fully with the CO regarding any matters associated with compliance with the AML &CTF laws and regulations.

4.6 Counter staff

Our counter staffs deal with our customers and accept instructions for transactions and they are responsible for:

- Following the identification and verification procedures in this manual;
- Completing transactions in accordance with the procedures in this manual and in other procedures for our business;
- Reporting any breaches of identification and verification procedures to the CO;
- Reporting any signs of unusual, suspicious or illegal activity by customers to the CO;
- Attending all AML & CTF training sessions that are scheduled.

4.7 Operations

Our operations staff process transactions and perform other activities associated with our business and they are responsible for:

- Following the procedures in this manual;
- Completing transactions in accordance with the procedures in this manual and in other procedures for our business;
- Reporting any breaches of identification and verification procedures to the CO;

5. TRAINING/AWARENESS

5.1 New Staff, Employee

5.1.1. The compliance officer will ensure that all new staff members or employees are trained and made aware of this manual before they commenced handling customers and transactions.

5.2 Existing Staff, Employees

5.2.1The compliance officer will ensure all staff members or employees attend AML&CFT training at least annually.

5.3 Training Records

5.3.1 Records will be kept of the following for 6 years from the date that training was provided:

- Who was trained;
- What material they were trained with;
- The attendance logs signed by attendees;
- The date they were trained.

6. CUSTOMER ACCEPTANCE PROCEDURES

6.1 Description of our identification and verification process

6.1.1 An individual who wants to establish a business relationship with us is an "Applicant".

6.1.2 Our application form is designed to capture all the information we need to be able to:

- Establish the identity of the Applicant;
- Assess the risk presented by the application and the Applicant;
- Complete special transactions such as those that involve sending or receiving money from overseas or are above $1 million or its equivalent in foreign currencies.

6.1.3 Applicants must complete and sign the application form which applies to the transaction they want to do and successfully complete our identification and verification procedure. The purpose of the identification and verification procedure is to reasonably be satisfied that the Applicant is who they claim to be and also to help us understand what risk they represent to us of being involved in money laundering or terrorism financing.

6.1.4 Where an Applicant cannot successfully complete and sign our identification and verification procedure their application must be refused and the matter reported immediately to the CO.

6.1.5 The CO will decide whether the inability to successfully complete our identification and verification procedure should be reported.

6.1.6 The Applicant must not be informed of the reporting of the matter to the CO or what decision is made about reporting the matter. Failure to comply with this procedure may be a criminal offence.

6.2 Identification information

6.2.1 All Applicants who are individuals must provide at a minimum the following information on their application form:

- Their true and full name and if they use more than one, all of their names;
- Their date of birth;
- Their occupation;
- Their permanent residential address;
- Their purpose and intended nature of the business relationship with the reporting entity;

Authorization of any person purporting to act for or on behalf of the customer and the identity of the person

6.2.2 All Applicants must sign their application form with their usual signature and where an automated sales receipt is used, they should also sign this receipt.

6.2.3 All Applicants who are Legal persons as customer and for a Legal arrangement as customer the reporting entity would collect the customer information:
(i) The purpose and intended nature of the business relationship with the reporting entity;
and (ii) The customer's beneficial ownership and control structure

6.3. Verification information

6.3.1 Our counter staff are required to verify the identification information using reliable and independent documents. On receiving the application form the counter staff must then ask for the following:

- At least one photographic verification document and at least one non-photographic verification document;
- Any two of either Category A documents (see AML & CTF Regulation Order).

6.3.2 We accept alternative documents if the Applicant cannot produce either the passport or driver's license:

- One category A document and two category B letters;
  or • Three category B letters.

6.3.3 If a photographic verification document is unattainable and if so proven then at least 3 non-photographic verification documents is satisfactory.

6.3.4 We do not accept the application of an Applicant that fails to produce photographic identification on more than three occasions unless there are reasonable grounds to believe that they do not possess any document which contains photographic identification. This will only arise in a small number of isolated cases where people are older or live in remote areas.

6.3.5 The documents produced by the Applicant for verification of their identity must then be used for the following comparisons:

- Whether the photograph on the document is of the same person as the Applicant;
- Whether the name on the document is the same as provided by the Applicant on the application form;
- Whether the date and place of birth on the document is the same as provided by the Applicant

on the application form;

- Whether the address on the document is the same as provided by the Applicant on the application form (addresses on passports are often different because people do move addresses).

6.4 Discrepancies

6.4.1 If the photograph, name or date or place of birth on the document is different to the application form then the Applicant should be asked for an explanation. If the explanation is not sufficient then the application should be refused and the matter reported to the CO.

6.4.2 If the name on the document is different to the name on the application because the person has changed their name through deed poll or through marriage then the Applicant must produce their deed poll for change of name or their marriage certificate.

6.4.3 Differences in dates of birth and places of birth should be reported to the CO before accepting the application.

6.4.4 Differences in appearance between the photograph on the document and the Applicant's appearance should be reported to the CO before accepting the application.

6.5 Local knowledge

6.5.1 Counter staff who know Applicants personally, or they or someone else in our office may have akin relationship with the Applicant, must still always require those Applicants to successfully complete the identification and verification procedure, including production of current and valid identification documents.

6.5.2 Applicants who are publicly well known because they are prominent public persons are still required to successfully complete the identification and verification procedure, including production of current and valid identification documents.

6.5.3 Counter staff should go to the CO if they are experiencing difficulties with this part of our procedures.

6.6 Record making and keeping

6.6.1 The documents produced to verify identification will be photocopied and stored with the application.
Each copy identification document will be stamped or noted with the following words "Original cited [date] by [name]" and the stamp or note initialed by the counter staff person completing the identification and verification procedure. Note – this could be set up on a stamp for staff to use.

6.6.2 The reverse side of the application form needs to be completed by the counter staff to complete the identification and verification procedure and it includes a statement explaining the reasons where only Category B documents have been accepted for verification.

6.7 Persons acting as agents for Applicants who are individuals

6.7.1 Where an Applicant does not attend our office in person but sends someone to present the application and perform the transaction for them then the steps below must be completed. The reasons this might occur include:

- Poor mental or physical health;
- Geographical remoteness; or
- Advanced age.

6.7.2 The person representing the Applicant needs to provide written authority of the basis on which they represent the Applicant. This authority must be an original document, not a copy. Usually it will be a letter written to our business confirming permission to perform the transaction in the application and signed by the Applicant.

6.7.3 The application must be accompanied by certified copies of the Applicant's identification documents. The person certifying the documents must be a suitable person such as a lawyer, accountant, commissioner of oath or manager of a domestic bank. The certified document must include a statement that the certifier has compared this copy document with the original and certifies that it is a true copy and provide details of the certifier's name, position and contact address and telephone number.

6.7.4 For all transactions over $1 million or its equivalent in foreign currency, the counter staff will call the certifier and confirm that they did certify the identification documents.

6.7.5 For all transactions over $10 million or its equivalent in foreign currency, the counter staff will try to contact the Customer and verify the transaction. If the Customer cannot be contacted then a letter will be sent confirming the transaction to the Customer's address.

6.7.6 Where there are repeated transactions by an Customer who does not attend our office then unless they are physically unable to attend the matter should be reported to the CO who will decide whether to permanently refuse such transactions unless the Customer attends in person with their identification documents and subjects themselves to our identification and verification procedure.

6.8 Persons doing transactions in their own name on behalf of a third party

6.8.1 Each application form asks the Customer to confirm that this transaction is being done by them for their own benefit and using their own money.

6.8.2 If an Customer says that the transaction is for another person or uses money from another person then the application must be made by that other person and they must successfully complete our identification and verification procedure.

6.9 Exception Register

6.9.1 As there are problems with identity documentation the CO keeps an Exception Register of persons who have difficulty in easily producing these documents regularly or who are unable to attend in person because of their health, remote location or age. Counter staff may use this Exception Register to establish verification of identity for these Applicants.

6.9.2 The CO will keep the following information in the Exception Register:
- Full details of the Applicant's identification information;
- A record of the verification documents used to establish identity;
- A record of the reasons why producing this information for each application is difficult.

6.9.3 The CO will review Applicants in the Exception Register every three years to confirm that their identification information is current.

6.9.4. The Exception Register cannot be used for higher risk Applicants or for transactions in excess of $400, 000.

6.10 On-going due diligence Process

6.10.1 An Applicant who has satisfied the identification process (and verification process) and has established a business relationship with us is now known as a "Customer".

6.10.2 Transaction Monitoring Process whereby transactions or attempted transactions are monitored so to identify any suspicious, complex, unusual, and have no apparent visible economic or lawful- purpose transaction. The transaction monitoring system will search transactions that are conflicting with the information held about the business relationship with the reporting entity.

6.10.3 Customer Monitoring Process where the relationship of the business with its customer is monitored to ensure that the customers activities being conducted are consistent with the business knowledge of the customer, the customer's business, source of funds and risk profile.

7. AML & CTF CONTROLS

7.1. Special Transaction Controls

7.1.1 We have the following transaction types:

- Purchase of money orders
- Purchase of traveller`s cheques
- Cashing money orders
- Cashing traveller`s cheques
- Sending money to another person
- Receiving money for a person from someone else
- Sending money to another person overseas
- Receiving money for a person from someone else overseas
- Exchanging $ for foreign currency
- Exchanging foreign currency for $
- Exchanging one foreign currency for another foreign currency.

7.2. Application forms are different for different transactions

7.2.1 Counter staff must ensure that the correct application form is used for each transaction. Each form has been designed to get the right information from the Applicant.

7.2.2 All Applicants must complete all the required information fields on the application form which applies to their transaction.

7.2.3 Staff must not accept incomplete application forms.

7.2.4 Where an Applicant insists that they cannot provide all the information requested, or the

information provided does not make sense then their application should be referred to the CO for her approval.

7.2.5 The CO will decide whether the absence of certain information or the nature of the information is such that the transaction can still proceed, alternatively whether it should be refused and the application reported.

7.2.6 If the application is refused by the CO then the Applicant must not be informed about what decision was made about reporting the matter. Failure to comply with this procedure maybe a criminal offence.

7.2.7 Counter staff and Operations staff are responsible for checking that the information provided on each application makes sense. They cannot ignore other information they may know about the Applicant or the transaction just because it is not on the application form.

7.3. Compliance with these procedures

7.3.1 No transaction may be completed unless all the information required has been provided. However the CO does have power to over-ride this in limited circumstances.

7.3.2 Counter staff repeatedly accepting transactions without all the required information will be subject to disciplinary action and potential dismissal.

7.3.3 Counter staff must be careful to insist on provision of all the required information even though they or someone else in our office may have a kin relationship with the Applicant.

7.3.4 Counter staff should go to the CO if they are experiencing difficulties with this part of our procedures.

7.4 Enhanced Identification and Verification process

7.4.1 Staff who become aware of the status of an applicant or customer that he/she occupy and is defined as someone listed under 8.1 or the beneficiary of a transaction as someone listed under 8.1, must immediately inform the CO.

7.4.2 Our CO must, in addition to the normal identification and verification process,

- collect additional information on the applicant (volume of assets, information available through public domain)
- collect additional information the intended nature of the business relationship
- collect information on the source of the funds or source of wealth
- collect information on the ultimate beneficiary
- Obtain the senior management's approval to commence the business relationship.
- Request the applicant/customer to carry out the first transaction/payment to be carried out through a bank account under the customer's name

7.4.3 Our CO will keep records of all his findings and the senior management decision.

7.5 Enhanced On-Going Due Diligence Process

7.5.1 Staff must immediately inform our CO of any and all transactions conducted by a customer listed under 8.3 or 8.4.

7.5.2 Our CO must, in addition to information collected earlier:

- Collect satisfactory information on the ultimate beneficiary of the transaction and on whose behalf the transaction was conducted
- Collect satisfactory information on the source of the fund in relation to the transaction
- Collect satisfactory information on the intended reason for the transaction
- Obtain the senior management approval for the transaction

7.5.3 Our CO must conduct strictly 3-monthly monitoring on our relationship with persons posing some level of AML&CTF risk and regularly update our information on such person's identification and verification including id documents (data).

7.6 Correspondent Banking

7.6.1 When our business engages the services of or has relationships with a cross border correspondent bank we must:

- Adequately identify and verify the person with whom we conduct such a business relationship with
- Gather sufficient information about the nature of the business of the person
- Determine from publicly available information the reputation of the person and the quality of supervision the person is subject to
- Assess the person's anti-money laundering and terrorist financing controls
- Obtain approval from senior management before establishing a new correspondent relationship
- Record the responsibilities of our business and the person whom we will engage business with.

7.6.2 Should the customers of the correspondent bank wish to establish accounts with our business we must ensure that the person:

- Has verified the identity of and is performing on-going due diligence on their customers who make interested in engaging our services
- Is able to provide to us customer identification data of their customers whom they have referred to our business for use of our services.

8. RISK

8.1 Applicants and Customers

Applicants and applications received must be assessed on the level of AML&CTF risks they may impose on our entity and all transactions over a 400,000$ threshold conducted by said customers requires on-going CDD.

8.1.1 Introduced Applicants/Customer

Applicants or customers who are introduced to the business by our intermediaries or third party introducers and did not appear in person in the customer acceptance process must be subject to

the requirements under section 7.4 and 7.5

8.1.2 Applicants/Customers wishing to use high risk products/services or use high risk delivery method

Applicants or customers who are deemed as 'low risk' but wish to engage our services/products which we deemed as 'high risk' or delivery methods which are deemed as 'high risk' are subject to the requirements listed under section 7.4 and 7.5.

8.1.3 Customers with adverse financial report against them

Customers with adverse reports against them are subject to the requirements listed under section 7.4 and 7.5

8.1.4 Customers representing or are legal entities/arrangements

Customers representing or are legal entities/arrangement are subject to the requirements listed undersection 7.4 and 7.5

8.2 Product/Service Risk

8.2.1 Large Principal Money Transfers (LPMT) (Money Remitters)

8.2.1.1 All applications for LPMTs must be made in person and contain:

- The amount of the transaction
- The currency
- Source of the funds
- Description of the origin of the funds
- Purpose of the transaction
- Sender's full name
- Sender's occupation
- Sender's means of identification and details of the identification document
- Receiver's full name
- Details of the relationship between Sender and Receiver
- Supporting documents such as invoices, purchase orders, contracts.

8.2.1.2 Applications for LPMTs are not accepted from people under the age of 18 years.

8.2.1.3 Once the application has been made the details cannot be changed.

8.2.1.4 The receiver must provide valid identification before the money can be paid.

8.2.1.5 All refused and incomplete applications should be reported to the CO who in turn should report them.

8.2.1.6 All applications for LPMTs must be approved by the CO who may also need to obtain the consent of the franchisor.

8.3 High volume transactions

Customers conducting high volume transactions (i.e. whether the amount of the transaction is significant above the in-house threshold or conducting several transactions which the sum total to an amount above the in-house threshold) are subject to the requirements listed under section 7.4 and 7.5.

8.4 Politically Exposed Person

8.4.1 We consider the following persons are persons who may pose some level of AML&CTF risk to the business:

- Person who is or has been entrusted with prominent public functions (e.g. Head of State and Prime Minister)
- Serving Government Minister
- Serving Member of Parliament
- Serving senior officials of political party
- Serving senior Military officials
- Serving senior judicial officials
- Serving senior executive members of state owned corporation
- Serving senior executive members of international organization
- Person who has been convicted of a criminal financial offence not less than 2 years
- Director of a legal person or legal arrangement who has been convicted of a criminal financial offence not less than 3 years

8.5 High Risk Business Relationship

8.5.1 We must categorize applicants with appropriate risk level.

High risk relationships, we must examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions and unusual pattern of transaction which have no apparent economic or lawful purpose.

8.5.2 High Risk Customer must be subject to the requirement listed under section 7.5 of the Procedures Manual

8.6 Higher risk countries

8.6.1 The following countries are considered high risk countries:

- Iran
- Burma/Myanmar
- Nigeria
- Democratic People's Republic of Korea (DPRK)
- Cuba
- Bolivia
- Ethiopia
- Ghana
- Indonesia
- Kenya
- Pakistan
- Sao Tome & Principe
- SriLanka
- Syria

- Tanzania
- Thailand
- Turkey

8.6.2 All applications from applicants originated or possess identification/verification documents from the high risk country must be forwarded to the CO for her and senior management's review and approval.

8.6.3 If the application is approved, the CO must conduct enhanced on-going due diligence on the applicant and transactions.

8.6.4 The CO must report any unusual matter.

8.7 Non-Resident Applicant

Non-resident applicants are subject to the requirements listed under section 7.4 and 7.5.

9. DECLINED BUSINESS

9.1 We do not accept business from the following people:

- Prescribed Money Laundering entity
- Prescribed terrorist organizations
- Serving inmates
- Minors (under the age of 16 years old)
- Customers operating under false or misleading names that we become aware of
- who does not produce identity or verification within prescribed timeframe

10. RECORD KEEPING

10.1 General

10.1.1 We need to keep records of our business to meet various legal requirements and ensure all transactions can be readily reconstructed at any time.

10.1.2 We also need to keep records of our identification and verification procedures and our transactions as well as other AML & CTF activities to comply with the requirements of the AML & CTF Act and Proceeds of Crime.

10.1.3 We keep our records in the English language.

10.2 Identification and Verification Procedures

10.2.1 All applications and documents produced to verify identity must be kept for a period of six years after the closure or termination of the account, service or business relationship.

10.3 Transactions

10.3.1 All records generated to complete a transaction should be filed with the application for the transaction and the documents produced to verify identity and the bundle must be kept for a

period of six years after the closure or termination of the account, service or business relationship.

10.3.2 For transactions, we generate and keep the following records:

- We give a reference number to the transaction;
- We record the currency the transaction is in;
- We record whether the transaction is inbound or outbound;
- We record the amount;
- We record the date of the transaction;
- We obtain and record the name of the Other Party;
- We keep the application and the identification documents, which also include the address and telephone details of the Customer;
- We keep any document the Customer has produced for the transaction such as an invoice.

10.4 Case Investigations

10.4.1 All case investigation files must be kept for six years after the date of the investigation.

10.4.2 All suspicious transaction reports to the VFIU must be kept for six years after the date of the report.

10.5 Governance and assurance documents

10.5.1 Documents generated to manage our AML & CTF obligations, such as this manual, or documents associated with a review of this manual, must be kept for a period of six years after the date of the report.

10.6 Retrieving records

10.6.1 All records kept must be able to be easily retrieved and in a form can read. Electronic records must be capable of being able to be printed out or read on screen.

11. REPORTING

11.1 Suspicious Transaction

11.1.1 Transactions or attempted transaction that are suspected to involve proceeds of crime or related to terrorist financing or conducted by prescribed entity or involved terrorist property or are unusual, complex, have no apparent or visible economic or lawful purpose.

11.1.2 Staff who encounters an unusual transaction or attempted transaction need to report it promptly to the CO and must not proceed further with the transaction unless the CO has given approval.

11.1.3 The staff must not inform the customer that the transaction or attempted transaction is unusual but must refer the Customer to the CO.

11.2 Suspicious Activity

11.2.1 Suspicious activity refers to a series of suspicious acts or transactions which are conducted overtime and form a pattern or trend.

11.2.2 Staff who encounters a suspicious activity or attempted activity need to report it promptly to the CO and must not proceed further with the activity/transaction unless the CO has given approval.

11.2.3 The staff must not inform the customer that the activity/transaction or attempted activity/transaction is unusual but must refer the Customer to the CO.

11.3 Large Cash Transaction

11.3.1 Counter staff must complete for all cash transaction exceeding $1 million or its equivalent in foreign currency and submit to the CO for her review and signoff.

11.3.2 The CTR must be submitted within: (a) for dollar currency -10 working days after the transaction or transfer is made; and (b) for foreign currency-2 days after the transaction or transfer is made.

11.4 International Currency Transfer

11.4.1 Counter staff must complete for all cross border fund transaction exceeding $1 million or its equivalent in foreign currency and submit to the CO for her review and sign off.

11.4.2 The IFTR must be submitted within: (a) for dollar currency -10 working days after the transaction or transfer is made; and (b) for foreign currency-2 days after the transaction or transfer is made.

11.5 Reporting process

11.5.1 Our CO is responsible for investigating what has been detected as unusual, deciding if something is suspicious and reporting it. Suspicion is personal, subjective and falls far short of the proof required for a criminal charge in a court. If the CO reports something that turns out not to be suspicious then he or she is protected under the AML & CTF ACT in respect of the report they made. The fact that a report has been made is confidential and no one outside and police and law enforcement will know that a report has been lodged.

11.5.2 Our CO will create a separate file for each investigation other than those which he or she decides on first reading are not suspicious. The CO will keep all the details of the investigation in this file and this file will be stored securely so no other staff can access it.

11.5.3 The CO may consider the following when investigation a transaction or an application:

- Is the size of the transaction consistent with the usual transactions of the Customer;
- Does the transaction make sense in the context of who the Customer is and what they do for a living?
- Has the pattern of transactions done by this Customer changed?
- Where the transaction involves overseas payments, is there a sensible reason why the Customer is engaging in the transaction?

11.5.4 When the CO decides that something is not suspicious, he will record his reasons in the file.

11.5.5 When the CO decides that something is suspicious, he must report the matter in writing within 2 working days after forming the suspicion. The Report must be in the prescribed form of

this manual.

11.5.6 Our CO must report the large cash transaction and international currency transfer under the prescribed form. For transaction, the report must be submitted within 10 working days after the transaction is made and for transaction in a foreign currency, the report must be submitted within 2 working days after the transaction is made.

11.5.7 Our CO will keep a register of suspicious transaction reports, recording the date it was lodged and other identifying information. This register will be stored securely so no other staff can access it.

11.6 Incomplete wire transfers

11.6.1 If we have a wire transfer that does not contain complete originator information – the name, address and account number of the remitter then we always report these as suspicious and wait for instructions on how to proceed.

11.7 Tipping off

11.7.1 Our staff are prohibited from discussing any unusual matter, cash transaction or international funds transfer they report to the CO with any other person within or outside our business unless they have the CO's consent to do so.

11.7.2 Our CO is prohibited from discussing any report or unusual matter they investigate, or what the outcome of their investigation was with any person within or outside our business except where they need to do so to complete their investigation, or if they need advice or assistance. This includes management and owners.

11.7.3 Our CO will send any staff person who reports an unusual matter a reminder about the prohibition of the AML & CTF Act on tipping off.

11.7.4 Our staff receives training regarding the prohibition of the AML & CTF Act regarding tipping off.

11.8 Requests

11.8.1 Our CO will provide any additional information that is requested as per of the AML & CTF Act.

11.8.2 In addition, our business will submit an AML & CTF Compliance Report when requested as per of the AML & CTF Act.

11.8.3 Our Procedures Manual would be submitted upon request as per of the AML & CTF Act.

11.8.4 Our Risk Assessment will be conducted and submitted upon request as per of the AML & CTF Act.

12. OTHER CONTROLS

12.1 Employee screening and monitoring

12.1.1 We only employ people who have the competence to do the job they are employed for.

12.1.2 We look for people with integrity to work in our business.

12.1.3 We monitor our employees for conflicts of interest between their outside life and the work they do in our business.

12.1.4 We have a [code of conduct].

12.1.5 We do not employ people with criminal records.

12.1.6 All our owners have had a police check and we require all our employees to have a police check.

12.1.7 Any transactions that our owners or employees wish to do through our business must be approved by the CO.

12.1.8 We monitor transactions done through our business by persons we know are family or friends of our owners or employees.

12.1.9 We regularly screen our management staff against of the AML&CTF Act.

12.2 Training

12.2.1 All employees must complete the training that we provide annually on this manual and on the requirements of the AML & CTF Act. The training should ensure that employees are aware of the AML& CTF Act, the Guidelines and the procedures in this manual.

12.2.2 Our training covers:

- The requirements of the AML & CTF ACT;
- The requirements of this manual;
- Their responsibilities;
- How to detect suspicious transactions;
- The prohibition on tipping off.

12.3. Assurance

12.3.1 The CO will monitor the business for compliance with this manual. This monitoring will include checking that:

- Applicants are being identified properly;
- Records are being kept;
- Staffs are attending training and reading compliance newsletters.

12.3.2 The CO will keep records of the checking processes including the dates on which the checking occurred.

12.4 Independent review

12.4.1 The CO will periodically arrange for this manual to be reviewed by an independent person for compliance and adequacy. The CO cannot do this review, nor can a member of her or his staff.

12.4.2 The report of the independent review will be provided to the owner as the CO and the CO will undertake required remediation actions identified in the report if they are practicable and appropriate.