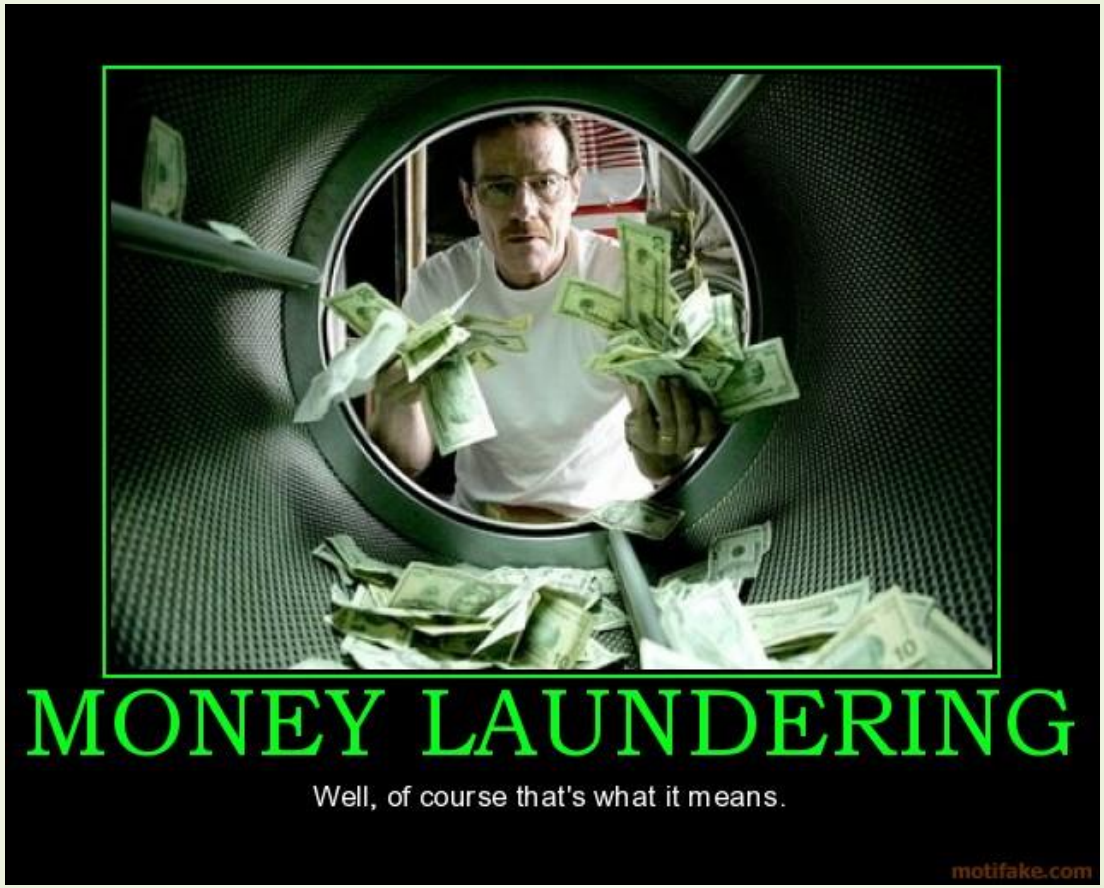
AML/CFT TRAINING FOR ACCOUNTANTS AND AUDITORS

16 MARCH 2016

BANK **USE PROMOTION & SUPPRESSION OF MONEY LAUNDERING UNIT**


MONEY LAUNDERING
Well, of course that's what it means.
motifake.com

What is Money Laundering?

- the process of **concealing** illicit gains from criminal activity;
- the process of **cleaning-up** dirty money;
- the process of taking the proceeds of criminal activity and making them **appear legal**;

Money laundering…

- For money laundering to take place, an **underlying offence** (referred to as the "**predicate offence**") would have been committed from which the criminal(s) derived a **financial benefit**.
- The person laundering funds may or may not have been directly involved in the underlying predicate offence.
- The offence of money laundering is criminalized under section 8 of the Money Laundering and Proceeds of Crime Act [Chapter 9:24], of 2013.

Why Launder Money?

Criminals want their illegal funds laundered so that they can move them through society freely, without fear of the funds being traced back to their criminal deeds.

Methods of Laundering Money

- There are various methods of laundering proceeds of crime, including transmitting such funds through the formal financial systems (e.g. Banks) and purchasing high value assets such as real estate, vehicles and investments in the securities market, among others.

Effects of Money Laundering

- Distorts investments and depresses productivity.
- Facilitates domestic corruption and crime, which in turn depresses economic growth.
- Reputational and Integrity Risks for Institutions.
- Nations where crime and corruption are prevalent investors are reluctant to invest

TERRORIST FINANCING

What is Terrorist Financing?

- Terrorist financing is the raising, moving, storing and using of financial and other resources for the purpose of terrorism.
- **Money** (*or its equivalent in other assets*)underpins all terrorist activities. Without it, there can be no training, recruitment, facilitation or support for terrorist groups.
- The disruption of terrorist financing is a key element in the overall fight against terrorism.

Terrorist Financing….

- Following the 2001 (9/11) terrorist attack in the USA that killed over 3000 people, the global anti-money laundering framework was expanded to enable it to deal with terrorism.

- In Zimbabwe, financing of terrorism is criminalized under section 9 of the MLPC Act.

THE INTERNATIONAL AML/CFT FRAMEWORK

FATF (financial action task force)

- **FAFT** is an inter-governmental body whose purpose is to establish international standards and promote national and international policies to combat money laundering (ML) and terrorist financing (TF).
- Established by the G-7 Summit in Paris in July 1989 to formulate measures to combat money laundering.
- Originally comprised the G-7 member States, the European Commission and 8 other countries.

FATF: Today

- 35 member countries + 2 member organizations
- 8 FATF-style regional bodies (FSRBs)
- 22 Observers .
- Over 190 countries have endorsed the FATF Standards

FATF…

- Core activities:

1) Setting Standards (FATF 40 Recommendations)
2) Assessing compliance by countries and their designated institutions
3) Identify and respond to ML/TF threats: high risk jurisdictions and typology studies

FATF assess compliance

- Countries are regularly assessed and are expected to address identified deficiencies within agreed timeline.

- The Recommendations are enforced by the FATF both on its membership and through a network of FATF-Style Regional Bodies (FSRBs) such as ESAAMLG, to which Zimbabwe is a member.

FATF-Style Regional Bodies

- Eastern and Southern Africa Anti-Money Laundering Group (**ESAAMLG**);
- Intergovernmental Action Group against Money Laundering in Africa (**GIABA**) (West Africa);
- Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (**MONEYVAL**) (European Union);
- Eurasian Group (**EAG**);
- Middle East and North Africa Financial Action Task Force (**MENATAF**);
- Asia-Pacific Group on Money Laundering (**APG**);
- Financial Action Task Force on Money Laundering in South America (**GAFISUD**);
- Caribbean Financial Action Task Force (**CFATF**)

FSRBs….

FATF-style regional bodies are an important extension of FATF work:

- Endorse and seek to implement FATF standards and modus operandi
- Observers at FATF meetings

International Institutions and Organisations

- IMF; World Bank – technical assistance, risk assessments
- United Nations – UNODC
- Basel – alignment of standards
- Interpol – law enforcement
- Egmont Group – international grouping of FIUs

Mutual Evaluations

All FATF members and FSRB members undergo regular Mutual Evaluation assessments:

- Purpose is to monitor compliance
- Provide analysis of deficiencies for remedial action
- Zimbabwe underwent evaluation by ESAAMLG assessors in 2015. Onsite visits, from 12 to 24 July 2015.

ZIMBABWE'S AML/CFT LEGAL AND REGULATORY FRAMEWORK

The AML/CFT Legal Framework

Zimbabwe's AML/CFT legal framework mainly consists of:

- **The Money Laundering and Proceeds of Crime Act [Chapter 9:24]**
- **The Bank Use Promotion Act [Chapter 24:24]**
- **Suppression of Foreign and International Terrorism Act [Chapter 11:21]**
- **Statutory Instrument 76 of 2014 (UNSCR 1267 , 1373, Successor Resolutions**
- **AML/CFT Guidelines for various institutions,**
- **Directives**

FINANCIAL INTELLIGENCE UNIT

F.I.U

FIU

- FATF Recommendation 29 requires every country to have a financial intelligence unit (FIU).
- Unit established in 2004 as a department within the central bank.
- Has a statutory mandate separate and independent from the Reserve Bank.

Main Roles of the FIU

(1) receives Suspicious Transaction Reports (STRs) and other financial data from financial institutions and DNFBPs;

(2) analyzes the received reports and data; and

(3) disseminates financial intelligence on suspected ML, TF and other crimes to appropriate law enforcement agencies, usually police.

(4) Gives feedback to reporting Institutions

(5) Coordinates all AML/CFT requirements with stakeholders

(6) Chairs the National Task Force and Anti-money Laundering Advisory Committee

(7) Prepares bi-annual reports to the Minister of Finance (June and December)

(8) Prepares reports for and advises the Governor

The FIU…

- The FIU has powers to levy monetary and administrative penalties against non-compliant / uncooperating designated institutions and /or their respective supervisory bodies.

Designated Institutions (DIs)

Are institutions that are subject to AML/CFT obligations, both in terms of The FATF Recommendations and the MLPC Act.

Categories of DIs:

- Financial institutions; and
- Designated Non Financial Businesses and Professions (DNFBPs)

Designated Institutions (DIs)…

- Financial institutions fall into two broad categories:
  - Banks; and
  - Non-bank financial institutions:
- **Non-bank** financial institutions include entities in the insurance, securities, microfinance institutions sectors.
- DNFBPs include: Legal practitioners; **accountants**; estate agents; casino operators and dealers in precious metals and stones
- DIs are "gatekeepers" to the financial system and the economy at large.
- They are required to put in place a broad range of AML/CFT measures to guide against ML/TF activities by their clients.

ZIMBABWE LAW ENFORCEMENT AGENCIES (LEAs)

The Unit works hand in hand with LEAs. Financial intelligence reports (*FIU output*), are forwarded to LEAs, for further investigations.

List of LEAs:

- ZRP
- ZACC
- ZIMRA
- IMMIGRATION

ACCOUNTANTS AND AUDITORS

- Accountants and Auditors are vulnerable to be used by clients or client counterparts, for ML/TF.
- Nature and duties carried out by these professions put them near the top of FATF list of institutions prone to abuse by money launderers and terrorist financiers.
- Their nature of duties, also put them at the top of the list of institutions who can **identify** and **report** ML/TF activities.
- These Institutions have the role to notify responsible authorities (FIU), of **illicit or suspicious transactions**.

AML/CFT Requirements for Accountants and Auditors

Key Requirements:

- Risk assessment and Implementation of the Risk Based Approach
- Customer Due Diligence (CDD, i.e. identifying customer and understanding the customer's nature of business and source of funds.
- Recordkeeping; transaction and customer records must be kept for at least 5 years.
- Suspicious Transaction Reporting (STR)
- Large cash transaction reports
- Implementation of UN Sanctions List
- AML/CFT internal programmes and controls
- Staff training

ML/TF Risk Assessment

FATF Recommendation 1:

Countries should **identify, assess, and understand** the **money laundering** and **terrorist financing** risks for The country, and should take action, including **Designating an authority or mechanism** to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively.

Based on that assessment, countries should apply a **risk-based approach (RBA)** to ensure that measures **to prevent or mitigate** money laundering and terrorist financing are **commensurate with the risks identified**.

Zimbabwe ML/TF National Risk Assessment

- In 2015, Zimbabwe undertook the NRA, which identified sectors of the economy which are highly vulnerable to MI/TF.
- Came up with a Detailed Actin Implementation Plan (DAIP), to address the identified risks.
- Supervisory Regulatory Authorities are now undertaking Sectoral MI/TF Risk Assessments for their sectors, in line with provisions of Recommendation 1.
- Designated institutions (accountants & auditors) will conduct their institutional ML/TF risk assessments.

Application of AML/CFT Risk Based Approach by Accountants & Auditors

- After identifying risks, designated institutions (DIs) are required to apply the risk based approach (RBA), in executing their AML/CFT measures.
- The RBA allows DIs to determine and implement proportionate measures and controls to mitigate these risks, cost effectively.
- Application of risk categories enables them to subject its customers/transactions to proportionate controls and oversight.

Application of RBA to AML/CFT…

- Once you have identified high risk customers, transactions, countries, geographical locations, there is need to apply enhanced customer due diligence.
- For low risk customers, designated institutions are allowed to apply simplified CDD.

High Risk Countries:

- Drug producing countries
- Countries linked to terrorist financing and activities
- Countries with high levels of corruption
- Countries on the FATF list of countries that are identified as not adequately implementing AML/CFT measures.

Transactions involving such jurisdictions are classified as high risk.

Examples of High Risk Customers/Transactions

- Nonresident customers;
- High net worth individuals;
- Politically exposed persons (PEPs);
- Transactions involving customers in multiple jurisdictions;
- customers from countries that do not or insufficiently apply the FATF standards

Controls for Higher Risk Situations

AML/CFT measures and controls to be taken for higher risk customers and transactions include:

- Increased awareness on higher risk customers and transactions from high risk jurisdictions.
- Increased levels of know your customer (KYC) or enhanced customer due diligence.
- Increased monitoring of transactions.
- Reporting of Suspicious Transactions
- Training & Awareness of staff

Politically Exposed Persons (PEP)

Enhanced Due Diligence shall be applied to PEPs, both local and foreign. FIs are required to:

- Obtain senior management approval for establishing a business relationship with a PEP;
- Take reasonable measures to establish the source of wealth and source of funds; and
- Conduct enhanced ongoing monitoring of the business relationship.

Enhanced CDD requirements for PEPs shall also apply to family members and close associates of such PEPs.

CUSTOMER DUE DILIGENCE & KNOW YOUR CUSTOMER (CDD/KYC)

Customer Due Diligence

- Both the FATF standards and the MLPC Act set out a series of measures that designated institutions, including the accountancy profession, must take to prevent ML/TF. These measures, known as **"preventive measures"**, have been designed to protect designated institutions from abuse, and help them to adopt adequate controls and procedures.

The three core elements of CDD:

- **"identification", "verification" and "monitoring"** of customers and transactions.

Customer Due Diligence (CDD) & Know Your Customer (KYC)

CDD Involves ;

- Identify and verify the customer's identity using reliable, independent source documents, data or information
- Identify the beneficial owner of the customer, in the case of companies, trusts, and similar entities
- Obtain information on the purpose and intended nature of the business relationship
- On-going CDD on the business relationship to ensure that the transactions being conducted are consistent with the designated institution's knowledge of the customer
- Perform enhanced CDD for higher risk customers, e.g. Politically Exposed Persons (PEPs)

CDD/KYC…

- CDD/KYC is intended to enable designated institutions to form a reasonable belief that it **really** knows the true identity of each customer.
- Designated institutions need to know the reason for the transaction, and the source of funds.
- Failure to verify the identity of a customer or **beneficial owner** as a result of the lack of CDD information should form the basis for reporting the transaction as a STR to the Unit.

CDD & KYC…

CDD requirements apply to accountants when they prepare for or carry out transactions for their clients concerning these and other activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies; or
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities
- company secretarial services

Suspicious Transactions

- A transaction which is **inconsistent** with a customer's known, legitimate business or personal activities

- It is a transaction which is **unusual** because of its nature, size, volume, or pattern

Accountants and Auditors are required to identify and report STRs to the Unit, immediately, but no later that 72hours.

Suspicious transaction “red flags”

- Client has a history of changing bookkeepers or accountants yearly/frequently
- Company carries non-existent or satisfied debt that is continually shown as current on financial statements.
- Company is paying unusual consultant fees to offshore companies
- Company records consistently reflect sales at less than cost, thus putting the company into a loss position
- Company is invoiced by organizations located in a country that does not have adequate money laundering laws and is known as a highly secretive banking and corporate tax haven.

AML/CFT Training & Awareness

- DIs are required to formulate and implement, on an ongoing basis, comprehensive employee education and training programs to equip employees with relevant AML/CFT skills.

Record Keeping

- All customer and transaction records should be maintained for at least five (5) years;
  - to enable compliance with information request from the competent authorities

Implementation of United Nations Sanctions List

(ISIL , Al Qaeda & Taliban Sanctions Lists)

Legal Requirements:

- UN passed resolutions UNSCR 1267 and 1373 which calls for all member states to identify and freeze assets of individuals or entities designated under the UN Al-Qaeda and Taliban Sanctions list.

- Zimbabwe ratified these resolutions by passing the Suppression of Foreign & International Terrorism Act, MLPC Act and Statutory Instrument 76 of 2014.

- SI 76 of 2014 lays down measures to be followed in implementing the UNSCR 1267 and 1373.

- The Unit issues Directives to designated institutions whenever an individual or entity is added or removed from the ISIL, Al-Qaeda or Taliban sanctions list.

Institutional Requirements

- Upon receipt of a Directive, designated institutions are required to confirm receipt and check whether they hold any assets or funds of the listed person.
- If you identify any funds, you are required to immediately freeze them and report to the Unit. If you do not, you are still required to file a Nil Return to the Unit.
- Designated institutions have an obligation to, at all times, to keep itself informed of, and act upon such changes as shall be published from time to time on the following UN websites: www.un.org/sc/committees/1267/aq_sanctions_list.shtmlwww.un.org/sc/committees/1988/list.shtml

Institutional Requirements…

- Designated institutions should put monitoring mechanisms in place (preferably IT based) which they use to check names of their customers and transacting partners against the UN Al-Qaeda and Taliban sanctions list, at all times.

AML/CFT Internal Framework should cover:

- Board & Management Oversight
- Policies & Procedures
- Human Resources & Training
- Management Information Systems (MIS)
- Internal Audits

Board Oversight

- The Board shall ensure that a comprehensive operational AML/CFT Policy Manual is formulated by management and presented to the Board for consideration and formal approval.

Failure to Comply with AML/CFT Legislations

Failure to Comply with AML/CFT Legislations

- Failure by DIs to comply with Directives issued from time to time, and the AML/CFT laws, attract administrative penalties, which the Unit now has powers to impose, in terms of section 5 of MLPC Act.

- Failure will lead to the country being classified as non complying with FATF international standards and UNSCR .

ICAZ's Responsibility

- The institute should ensure that its members comply with the country's AML/CFT legislations.

Questions?

THANK YOU