ANTI-MONEY LAUNDERING AND RISK ASSESSMENTS

By Louis Owoko, FCCA, CTP, CFM

ACT East Africa Conference

Villa Rosa Kempinski, Nairobi

13th March 2019

Money Laundering

- **Definition:** 'Money Laundering' is the process by which illegal funds and assets are converted into legitimate funds and assets.

- Illegal/Dirty Money is converted into legal/white money

Money Laundering

"Money Laundering is the conversion of profits from illegal activities into financial assets which appear to have legitimate origins."

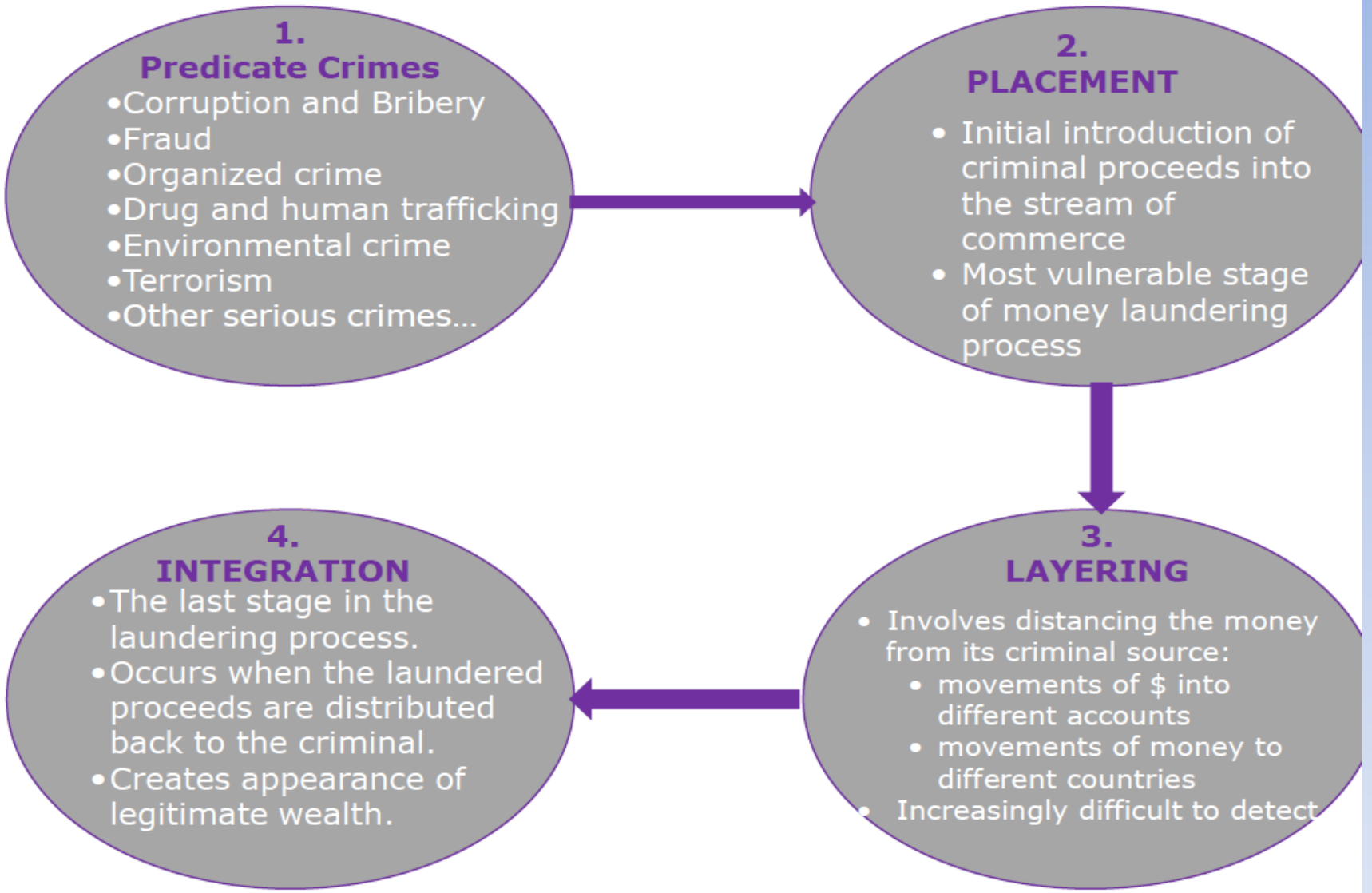
"Money laundering is any action taken to conceal, arrange, use or possess the proceeds of any criminal conduct" – Serious Organised Crime Agency, UK

Money Laundering- Stats

- According to the IMF, funds laundered in the world could range between 2-5% of the world's gross domestic product

Money Laundering generally refers to 'washing' of the proceeds or profits generated from:

Money Laundering Cycle:



Some of the Popular Places from where Money is laundered through…

- Stock Markets

- Agricultural Products (as there is no income tax and mostly the transactions are on cash basis)

- Property Market

- Creating Bogus Companies

- Showing Loans

- False Export Import Invoices

Terrorism Financing

Although terrorist financing is a form of money laundering, it doesn't work the way conventional money laundering works. The money frequently starts out clean i.e. as a 'charitable donation' before moving to terrorist accounts. It is highly time sensitive requiring quick response.

Money laundering Risks

(i) Reputational risk

(ii) Legal risk

(iii) Operational risk

(iv) Concentration risk (either side of bal sheet).

- All risks are inter-related and together pose a serious threat to the organization's survival

Reputational Risk

- The potential that adverse publicity regarding an institution's business practices, whether accurate or not, will cause a loss of confidence in the integrity of the institution.
- Its a major threat to organisations as confidence of customers, suppliers and general market place is affected.

Operational Risk

The risk of direct or indirect loss resulting from inadequate or failed internal processes, people, technology and systems or from external events.

Weaknesses in implementation of programs, ineffective control procedures and failure to practice due diligence

Legal Risks

- The possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of an institution.
- Banks in particular may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practice due diligence.

Concentration Risk

- Mostly applies on the assets side of the balance sheet: Information systems to identify credit concentrations; setting prudential limits to restrict banks' exposures to single borrowers or groups of related borrowers.
- On liabilities side: Risk of early and sudden withdrawal of funds by large depositors- damages to liquidity.

Risk Assessments - KYC

Customer?

One who maintains an account, establishes business relationship, on who's behalf account is maintained, beneficiary of accounts maintained by intermediaries, and one who carries potential risk.

Know? What you should know?

True identity and beneficial ownership of the accounts. Permanent address, registered & administrative address

What KYC means

- Making reasonable efforts to determine the true identity and beneficial ownership of accounts;
- Sources of funds.
- Nature of customers' business.
- What constitutes reasonable account activity?
- Who your customer's customers are?

Elements of KYC

- Customer Acceptance Policy.
- Customer Identification Procedure- Customer Profile.
- Risk classification of accounts
- Ongoing monitoring of account activity.
- Reporting of cash and suspicious transactions

Deterring money laundering

- Board and management oversight of risks
- Appoint a senior executive as principal officer with adequate authority and resources
- Systems and controls to identify, assess & manage the money laundering risks.
- Appropriate documentation of risk management policies, their application and risk profiles.

Deterring money laundering...

- Appropriate measures to ensure that ML risks are taken into account in daily operations, development of new financial products, establishing new business relationships and changes in the customer profile.
- Screening of employees before hiring and of those with access to sensitive information.
- Appropriate quality training to staff.
- Quick and timely reporting of suspicious transactions

Role of cash in ML

- Disguises the audit trail.
- Provides anonymity.
- Conceals true ownership and origin of money.
- Control over money.
- Changes the form of money.

Requirements for Mobile Payment Services

A Mobile Payment Service Provider or its agent shall meet the following requirements to reduce the risk of mobile payment products being used for money laundering or terrorist financing

Requirements for MPS

a) Set transaction or payment account limits

i. Max Daily Transaction is Ksh **140,000**.

ii. Max transaction amount is Ksh **70,000**

iii) Max Account holding of Ksh **100,000**

b) Photo Identification of applicants using valid passports, national ID, Military IDs, Diplomatic ID, Alien ID or foreigners certificate

Requirements for MPS

c) Mobile payment accounts shall be opened using valid identification documents only. The Mobile Payment Service Provider should link the different accounts held by a single account holder and keep records of the same

Mobile ML Systems and Control

(a) Mobile Payment Services providers are responsible for managing operational risks through laid down procedures and controls by enforcing monitoring and reporting of suspected money laundering activities, verification of customer identity, documentation of customer records and establishment of internal reporting procedures.

Mobile ML Systems and Control

(b) Mobile Payment Services providers are obligated to put in place strong operational procedures and controls to handle and resolve customer complaints. This includes and is not restricted to, recording of sufficient transaction details to create an audit trail and storage of records for a minimum period of seven years from the date of transaction.

Mobile ML Systems and Control

(c) Mobile Payment Services providers must have clear accountability for actions of agents through agent agreements. Mobile Payment Services providers should verify, on a regular basis, compliance with policies, procedures, and controls as stipulated in the agreements, in order to ensure that the requirement to maintain such procedures has been discharged by their agents

Mobile ML Systems and Control

(d) If a Mobile Payment Service Provider or its agent becomes aware of suspicious activities or transactions which indicate possible money laundering or terrorism financing, the Mobile Payment Service Provider shall ensure that it is reported to the Financial Reporting Centre (FRC) immediately and in any event within seven days of the date of the transaction or occurrence of the activity that is considered suspicious.'

POCAMLA

Proceeds of Crime and Anti-money Laundering Act (POCAMLA) of 2009. It provides details for

- Reporting requirements
- Penalties
- Money laundering offenses.
- Establishment of the FRC, charged with receiving Suspicious Transaction Reports (STRs).
- Requirements for the tracing, freezing, and seizing of criminal proceeds

POCAMLA Amended 2017

- The Act recommends that a person who fails to comply with the law be liable to a fine of not more than Ksh5 million ($50,000), while the penalty for an institution will not exceed Ksh25 million ($250,000).
- The new legislation also formalises the establishment of the Assets Recovery Agency, which will handle all cases of recovery of the proceeds of crime that come from money laundering

Firm-wide risk assessment

Purpose

- Is robust enough to support risk based approach to managing ML/ TF risks.
- Takes inventory of risks and other relevant factors.
- Assists in implementing effective mitigation measures

Firm-wide risk assessment

- Should identify, assess, monitor, manage and mitigate the risks associated with ML and TF.
- Must be documented
- Senior management to provide policies, controls and procedures
- The assessment should identify business areas most at risk and focus resources to mitigate these risks

Steps in risk assessment

- Step 1: Identify the ML risks faced by different areas of the business, and the clients and markets served
- Step 2: Consider the likelihood and resulting impact of the identified risks
- Step 3: Review the mitigating checks, systems and controls

Risk Factors/Categories

Identifying and assessing ML/TF risks associated with unique combination of

- Clients/customers
- Products and services
- Countries that your clients operate in (Geographic locations)
- Transactions you are involved in
- Delivery channels

1. Customers Risk

Identify all categories of customers served, business relationships and assess AML risks (Risk posed by a customer)

Factors to consider

- Cash intensive businesses
- Customers whose structure makes it difficult to identify true owner

Customers Risk

- Those conducting businesses in unusual manner
- Foreign and domestic NGOs

Mitigations

- Enhanced Client Due Diligence (CDD)
- Senior management approval at take-on
- Frequent update of CDD

2. Products and Services Risk

Consider your services and how they can be used to launder money, conceal or layer ML

Factors to consider

- Categories of turnover on annual return
- List of services on website/promotional paper
- Organisational structure of the firm
- Is it a trust/company
- Are Payroll or insolvency services involved?

Products and Services Risk

Mitigations

- Stop offering services that are high risk
- Enforce a second-partner review for certain service types
- Compliance reviews of high risk services to ensure implementation of policies and procedures

3. Geographic Risk

- Where clients are based, obtain their funding, sell their goods/services, buy raw materials or how they are linked to countries through networks, agencies or suppliers
- Corrupt countries
- Those on sanction or embargo list by UN, FATF
- Those supporting terrorist activities/orgs

Mitigations

- Deal with Countries known to have effective AML regimes

4. Transactions you are involved in

- Applicable to those who operate clients money accounts. Assess the transactions that pass through these accounts. Payroll and insolvency services could be used to support criminal activities
- Are fees routinely remitted in cash?
- Are client's payments received from 3rd parties
- Firms providing a one-off transaction/service
- Active management over clients own accounts

4. Transactions you are involved in

Mitigations

- Consider the regulatory framework within which the transactions are facilitated
- Confirm the ultimate beneficiaries/owners

5. Delivery Channels Risk

- Consider all the methods of interaction with customers and how products/services are distributed. Some channels increase risk since they make it difficult to determine customer's identity

Factors to consider

- Face to face interactions, online correspondence, referrals, use of intermediaries and agents

Delivery channels

Mitigations

- Take on clients you have met face-to-face
- Thorough CDD
- Frequent update of CDD for clients not met

ML risks assessment

- Consider likelihood of risk occurring as well as the impact (likelihood vs impact matrix)

  Possible ranges for likelihood

- Almost certain(All but exceptional cases)
- Probable (Most cases)
- Possible (should occur some time)
- Unlikely (may occur some time)
- Rare

Impact

- Critical (Significant sums and may lead to potential criminal prosecution)
- Major (large sums with significant reputational damage to company)
- Significant (Moderate sums with reputational damages)
- Minor (limited sums with negligible reputational impact)

Mitigations - Summary

- Design effective Client Due Diligence (CDD)
- Enhanced CDD with frequent reviews for high risk factor areas
- Regularly screen staff involved in higher risk areas (internal AML and client take-on)
- More detailed and frequent training for staff working in high risk business areas

Mitigations - Summary

- Encourage MLRO to connect with other professionals or groups so as to keep abreast of new and emerging risks
- Establish checks to assess and frequently review higher risk engagements
- In extreme cases, terminate the high risk service or end the client relationship

Questions and Answers