Financial Crime Compliance

ILCA Masterclass, September 2020

Michael Heider / Head of Compliance, Paystack

Agenda

1. Definitions

Money Laundering

Terrorist Financing

What is Money Laundering

- Money laundering is the process of **making large amount** of money generated by a criminal activity, such as drug trafficking or terrorist funding, **appear**ing to have come from a **legitimate source**.

- Money laundering itself is a crime.

- There are **two main reasons** why criminals - whether drug traffickers, corporate embezzlers or corrupt public officials - engage in money laundering:
  - the money trail is evidence of their crime and
  - the money itself is vulnerable to seizure and has to be protected.

Three Stages of Money Laundering

Money-laundering is a dynamic **three-stage** process that requires:

(1) Placement:

- The placement stage represents the **initial entry** of the "dirty" cash or proceeds of crime into the financial system.

It is during the placement stage that money launderers are the **most vulnerable** to being caught. This is due to the fact that placing large amounts of money (cash) into the legitimate financial system may raise suspicions of officials.

Three Stages of Money Laundering

(2) Layering:

- After placement comes the layering stage. The layering stage is the most **complex** and often entails the international movement of the funds. The primary purpose of this stage is to **separate** the illicit money from its source. This is done by the sophisticated layering of financial transactions that obscures the audit trail and severs the link from the original crime.
- During this stage, for example, the money launderers may begin by **moving** funds electronically from one country to another, then divide them into investments placed in advanced financial options or overseas markets; constantly moving them to elude detection.

Three Stages of Money Laundering

(3) Integration:

- The final stage of the money laundering process is termed the integration stage. It is at the integration stage that the money is **returned** to the criminal from where seems to be the **legitimate** source.
- There are different ways in which the laundered money can be integrated back with the criminal.

For example, the purchases of property, art work, jewellery, or high-end automobiles are common ways for the launderer to enjoy their illegal profits without necessarily drawing attention to themselves.

What is Terrorist Financing?

- Terrorists and terrorist organizations also rely on money to sustain themselves and to carry out terrorist acts.
- While terrorists are not greatly concerned with disguising the origin of money, they are concerned with **concealing its destination** and the purpose for which it has been collected.
- Terrorists and terrorist organizations therefore employ techniques similar to those used by money launderers to hide their money.
- Money for terrorists is derived from a wide variety of sources. Compared to money laundering, money for terrorists **don't** necessarily **have** their **origin in criminal activities**.

2. Customer Due Diligence

Identification – Ascertaining and Verifying

Beneficial Ownership

Identification – Ascertaining and Verifying

- Identification is divided into two steps:
  - **ascertaining** the identity; and
  - **verifying** the identity.

- **Ascertaining** the identity means obtaining information on the identity of the natural or legal person to be identified.

- **Verifying** the identity means validating the information on identity obtained against meaningful supporting documents and information.

- Information on identity must be **documented**.

Information on identity

Natural Person:

- First Name
- Surname
- Gender
- Date of Birth

Legal Person:

- Company Name
- Legal Form
- Country of Registration
- Registering Authority
- Registration Number
- Place of Incorporation
- Purpose of Business
- Management bodies and authorised persons
- Beneficial Owner

Acceptable Photo Identification

- An **official photo identification document** is a meaningful supporting document for verifying the information on the identity of a natural person.

- An official photo document:
  - is a document that has been issued by a government authority;
  - bears a non-replaceable, recognisable photograph of the head of the person to be identified; and
  - the name of the person to be identified; and
  - the date of birth of the person to be identified; and
  - the signature of the person to be identified; and
  - the authority which issued the document.

Proof of Address

- Every natural person has to provide proof of their residential address as part of the KYC process.

- Proof of Address can be any personalised document from a company subject to AML regulations (e.g. Banks, Insurances, etc.), such as
    - Bank or Credit Union Statements
    - Credit Card Statements
    - etc.

Proof of Address

- Proof of Address can also be any personalised document from a company delivering permanent services into the residential address of the person to be identified, such as
  - Utility Bills (Water, Gas, Electricity, etc.)
  - Landline telephone/Internet/Cable TV Bills
  - NOT: Mobile Phone Bills

- Proof of Address must not be older than 6 months on the day of Identification.

Verifying – Legal Person

Meaningful supporting documents for the purpose of verifying the identity of legal persons are;

- **Certified extracts** (most recent version) from, e.g., commercial registers or, depending on the jurisdictions;
- **Company documents**, such as
  - Memorandum of Association
  - Articles of Association
  - Company Statutes
  - Certificate of Incorporation
  - Other documents, data or information stemming from a credible and independent source.

Verifying of Management Bodies

Information on management bodies (e.g. Directors, Company Officers, etc.) and other persons authorised to represent the company is verified according to the verification process of natural persons.

Beneficial Owner

- In general terms, the beneficial owner is/are the natural person(s) who **ultimately own(s) or control(s) the customer**.
- The beneficial owners of a company can only take the form of natural persons who:
  - hold sufficient large direct or indirect participation in the company;
  - hold sufficient voting rights either directly or indirectly in the company; or
  - exercise control over the management of the company in a different way.
  - Sufficient participation/ voting right exists when the natural person holds more **than 25% of the shares** or voting rights.
  - Whether a sufficient participation exists must be reviewed **at each level** and

3. Simplified Customer Due Diligence

Application of SDD

Application of SDD

- **Governmental Authorities and Public Bodies**
  (bodies of a legal law governed by public law)
  - incl. state authorities and every body of the state legislative, executive and judiciary powers

- **Stock Exchange-Listed Companies**

- **Credit and Financial Institutions** under governmental supervision

4. Enhanced Customer Due Diligence

Higher Risk of Money Laundering

Politically Exposed Persons

Complex Ownership Structures

Risk Mitigating Controls

Mandatory cases of EDD

- Enhanced Customer Due Diligence must be applied on a
  - Risk-sensitive basis

- Enhanced Customer Due Diligence must be applied in response to
  - Non face-to-face relationships
  - Relationships with ‘Politically Exposed Persons’ (PEPs)
  - Any other situation which by its nature can present a higher risk of money laundering

Politically Exposed Persons

- A politically exposed person
  - is a natural person from any state or third country
  - is or was up to one year ago entrusted with a prominent public function

  and
  - is an immediate family member or
  - is a person known to be close associate of such persons.

- In case a PEP has been positively identified to be involved in a business relationship, EDD will be triggered additionally.

Higher Risk of Money Laundering

Customer Risk Factors

- Unusual business relationship
- Cash-intensive business
- Bearer shares or Nominee shareholders
- Complex/unusual ownership structure

Product;
Service;
Delivery Channel

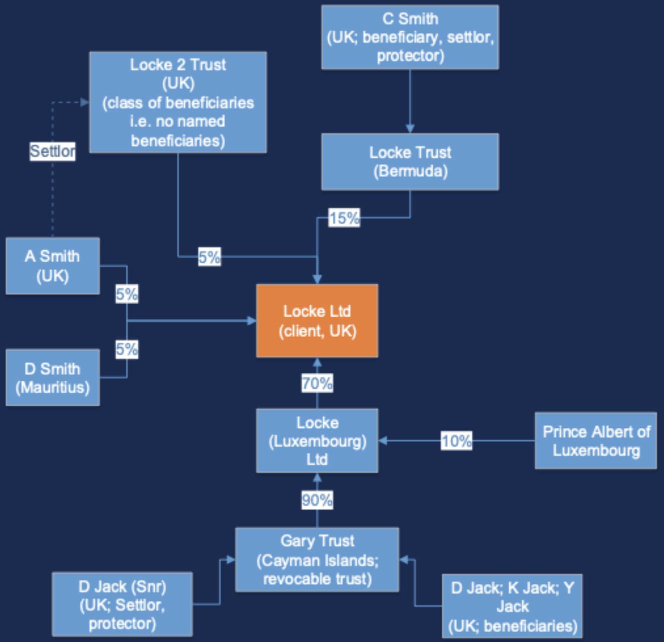
- Payments that will be received from unknown third parties
- Products or transactions with high anonymity
- Non-face-to-face relationships
- New products of business practices
- Nominee/shadow directors or company formed in 3rd countries

Geographical

- Countries without effective Anti-Money Laundering Systems;
- Countries with significant levels of corruption
- Countries subject to sanctions
- Countries providing funding/support to terrorist activities or with designated terrorist groups operating within their country

Complex Ownership Risk

- Lack of transparency, multiple levels of ownership, circular ownership



Ownership Structure and Beneficial Owner

- Why do we need to understand the ownership structure?
  - A clear picture of the ownership structure allows to identify the point of control where illicit money can enter the financial system
  - Keyword of beneficial ownership is control!
  - Full Identification and Verification is required for Beneficial Owners in order to demonstrate complete knowledge and understanding of who controls the flow of funds through the entity and into the system.

5. On-going Due Diligence

Risk-based Approach

KYC Refresh

What is On-going Monitoring?

- Financial Institutions have an obligation to monitor customers and their transactions on a continuous basis.

- They are expected to create a profile of the customer in order to manage risk.

- They should be able to analyse information obtained about their customer for consistency, reasonableness and new relationship development and compare what is known about the customer at on-boarding stage against how the customer is utilising the relationship.

What is On-going Monitoring?

- An On-going monitoring of business relationships involves:
  - Scrutinising the transactions to determine whether they are aligned to the intended nature and purpose if business relationship
  - Ensuring information collected as part of CDD/EDD is up to date and valid.

  This may be conducted on periodic review basis or driven by an event driven review.

Monitoring on a risk-based approach

The individual financial crime risk assessment defines specified time periods when monitoring should occur, but usually:

- High-risk customers: High risk clients will be subject to a higher frequency of monitoring; KYC refresh every year
- Medium-risk customers: Medium risk clients will be subject to lower frequency of monitoring; KYC refresh every 3 years
- Low-risk customers: Lower risk clients will be subject to the least frequency of monitoring; KYC refresh every 5 years

KYC Refresh

- KYC refreshes require checks whether there have been changes in;
  - Management Structure
  - Beneficial Ownership
  - Business Purpose
  - Transactional Profile
- Therefore, every Financial Institution is required to obtain
  - Updated documents (e.g. fresh extracts from the Commercial Register)
  - Copies of Identification Documents of new representatives of the company
  - Updated declaration on the Beneficial Ownership of the company (and, depending on the risk, collection of respective documents)

6. Sanctions and Embargoes

Purpose

United Nations

Special case: United States

About Sanctions and Embargoes

- Sanctions and embargoes are imposed on countries by the authority of the United Nations, its Member States and states applying extra-territorial jurisdiction (e.g. US).

- Sanctions and embargoes have direct impact on Financial Institutions.

- In some cases when special persons/ entities/ countries are under sanctions and embargoes, assets and resources have to be blocked or, in some cases, even abandoned.

Why are there Sanctions in place?

- Sanctions are measures taken by a state to coerce another to conform to an international agreement or norms of conduct, typically in the form of restrictions on trade or official sporting participation.

- Sanctions are a lower-cost, lower-risk, alternative to military force – and lie between diplomacy and war.

- Sanctions are sometimes used where military force is not feasible or where national interest are not directly threatened.

Excursus: US Sanctions

- As a general rule US sanctions apply:
  (i) within the territory of the United States;
  (ii) to US persons and entities whether or not they are in the territory of the US;
  (iii) trading in US goods and services (e.g. US Dollars).

- "US person" means:
  - Companies organized under U.S. law and their non-U.S. branches;
  - Employees of a U.S. company, as well as employees of its non-US branches
  - U.S. citizens or U.S. permanent residents, regardless of where they are located
  - Non-U.S. companies or people located in the U.S.

7. Monitoring and Screening

KYC Screening

Transaction Screening

Transaction Monitoring

KYC Screening

- Ongoing screening of all customers and their key parties against
  - PEP lists (both domestic and international and also their family and associated persons.
  - Sanction lists issued by
    (i) The United Nations
    (ii) The Home State and countries the Financial Institution is operating in
    (iii) States applying extra-territorial jurisdiction (e.g. US)

- Other information to highlight reputational risk exposure
  - Allegations of or convictions for financial crime
  - Business activities/practices that might raise concerns

Transaction Screening

- Ongoing screening of Payer information against
  - PEP lists
  - Sanction lists
  - Other information to highlight reputational risk exposure

Transaction Monitoring

- Transaction monitoring refers to the monitoring of customer transactions, assessing historical/current customer information (KYC profile) and interactions to provide a complete picture of customer activity.

- Transaction monitoring tries to monitor customers from various angles to detect ‘suspicious behaviour’ of money laundering and/or terrorist financing.
  - Real-time monitoring
  - Long-term monitoring (for transactional patterns)
  - Behavioural monitoring (transactions within customers profile)

8. Suspicious Activity Reporting

SAR Process and Violations

What is a SAR?

- A SAR is a document (electronic or other) that highlights a financial institutions concerns where they:
  - know; or
  - where they suspect; or
  - where they have reasonable grounds for knowing or suspecting that a person is engaged in, or attempting money laundering or terrorist financing.

- SARs 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 such as Terrorism.

SAR Process

1

Internal Reporting

report all unusual activity/transactions where there are reasonable grounds to suspect ML, TF or a Sanctions violation regardless of the amount of the transactions; whether or not the transaction was completed

2

Evaluation by MLRO

MLRO must consider each report and determine whether it gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion. The MLRO must have access to any information, about the customer or the transaction in the firm's possession which could be relevant. .

3

External Reporting

MLRO must report to the NCA as soon as is reasonably practicable any transaction or activity that, after his evaluation, he knows or suspects, or has reasonable grounds to know or suspect, may be linked to ML or TF, or to attempted ML or TF. This is done by submitting a Suspicious Activity Report (SAR).

Violations:

Tipping off is a serious criminal offence. You commit the offence if you make any disclosure likely to prejudice an investigation. Specifically, you must exercise care not to "tip-off" any individual that a potential case of money laundering has been escalated internally or is being investigated or disclosed externally i.e. the NCA. The offence can lead to 5 years imprisonment and/or unlimited fine.

9. Record Keeping

Retention periods

Record Keeping

- A Financial Institution is required to keep:
  - a copy of any documents and information obtained by a business to satisfy the customer due diligence requirements;
  - sufficient supporting records of all transactions to/from customers
- These records must be retained for a period of 5, sometimes 10 years from the time the relationship comes to an end or the completion of any occasional transaction.
- After the retention period has expired, all personal data must be deleted unless the Financial Institution is required to retain records containing personal data

  (i) by or under any enactment, or

  (ii) for the purposes of any court proceedings, or

  (iii) the customer has given express consent to the retention of that data.

Thank you for your time! ✌️ ♡

Michael Heider

Head of Compliance

Paystack

hello@paystack.com
@paystack
@paystackhq