1. Introduction

BII defines Money Laundering (ML) as the process by which the true origin and ownership of the proceeds of criminal activities are disguised in order to be used without suspicion. Money laundering takes many forms including:

- Trying to turn money raised through criminal activity into 'clean' money ('classic' money laundering)
- Handling income from acquisitive crimes such as theft, fraud and tax evasion
- Handling stolen goods
- Being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property
- Criminals investing the proceeds of their crimes in any financial products

For the purposes of this Toolkit 'money laundering' covers both terrorist and non-terrorist financing.

Money laundering is a global problem and frequently occurs across borders. Recent advances in technology and the increasing number of online business transactions have exacerbated the problem. Money laundering techniques are flexible by nature and can be easily adapted to the business environment of any jurisdiction. Money launderers often have vast resources at their disposal and receive professional assistance to carry out their activities. Countries with developing economies or those undergoing changes in their financial system are particularly vulnerable and can be lucrative markets for money launderers.

- The Money Laundering (AML) Process

  There are three recognised parts to a money laundering process:

  - **Placement**: This is the physical placement or depositing of cash derived from criminal activity into banks and other financial institutions such as currency exchanges. Deposited cash and assets are then converted into other financial instruments such as traveller's cheques, payment orders or are used to purchase

items for resale. Money launderers often use financial institutions in jurisdictions with weaker regulatory oversight and reporting standards on financial crime (e.g. FATF blacklist or grey list countries) where they deposit cash and then transfer it to banks in regulated environments as 'clean' funds.

- **Smurfing**: This is a form of placement where many small cash deposits are made instead of a single large one. Smurfing allows money launderers to evade local regulatory reporting requirements applicable to cash transactions. Cash-based businesses are an obvious point of entry into the financial sector for illegal funds.

- **Layering**: This is the separation of the proceeds of criminal activity from their source through the use of many financial transactions (layers). Layers may include multiple transfers of funds between financial institutions; cash collateralised loans and letters of credit with false invoices/bills of lading. The use of layers of financial transactions can disguise the origin of funds, disrupt any audit trail and provide anonymity. Money launderers seek to move funds around and change both the form of the funds and their location to make it harder for law enforcement authorities to identify 'dirty' money.

- **Integration**: This is the final part of the money laundering process and involves integrating laundered money back into the financial system in such a way that it re-enters as apparently legitimate funds that can be retained over the long term.

CLICK TO VIEW DIAGRAM

- Terrorist Financing (TF)

Terrorist financing is the provision or collection of funds with the intention that they should be used in full or in part, in order to carry out acts that are associated with the support of terrorists or terrorist organisations. There are a number of similarities between the movement of terrorist property and the laundering of criminal property – they both involve the movement of money or value (e.g. from one person/account to another) and are both used to disguise the source and destination of funds. Both regulators and FIs need to be alert to and understand the inter-relationship between the two crimes. However, there are two key differences between terrorist property

and criminal property:

- Often only small amounts are required to commit individual acts of terrorism. This increases the difficulty of tracking terrorist property e.g. buying cheap DIY equipment to build a bomb or hiring a car to commit a terrorist act.
- Terrorist organisations can sometimes be funded from legitimate income such as charitable donations. It is difficult to identify the stage at which legitimate funds become terrorist property.

Terrorist organisations usually require significant funding and large amounts of property to adequately resource their activities. Terrorist property and funds are often controlled via a number of sources and use modern techniques to manage funds and move them between jurisdictions without detection. A number of national governments and international organisations (including the UN) have created lists of organisations they designate as terrorist (designated terrorist groups). Some well-known terrorist organisations operating across multiple jurisdictions include: al-Qaeda, Al-Shabaab, Boka Haram, Islamic State of Iraq and the Levant (ISIL) and Hezbollah.

- Politically Exposed Persons (PEPs)

  Politically Exposed Persons (PEPs) are people who hold or have held (during the previous year) prominent public positions, either domestically or internationally. PEPs include:

  - Head of State or government
  - Senior politicians (e.g. Ministers and Deputy or Assistant Ministers)
  - Senior government, judicial or military officials
  - Senior executives of state-owned corporations or political party officials
  - Members of Parliament
  - Members of Supreme Courts, of constitutional courts, or of other high-level

judicial bodies

- Members of courts of auditors or of the Boards of central banks
- High-ranking officers in the armed forces.
- The family members and close associates of PEPs should also be treated as PEPs.

PEPs present heightened financial crime risk due to them typically being entrusted with a prominent public function presenting an increased risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold. However, the involvement of PEPs or their close family members and associates should not automatically stop a transaction from proceeding. The involvement of a PEP in a transaction instead should be regarded as an amber light and trigger enhanced due diligence, including understanding the position the PEP holds or held in a public institution (and potential for bribery & corruption – particularly in a country with inherent high corruption risk) alongside further checks to ensure their wealth has been legitimately generated. This may involve commissioning external enhanced due diligence reports from specialist financial crime/political intelligence firms to undertake detailed source of wealth and funds checks. Examples of such firms include Control Risks, Kroll, FTI consulting and Africa Practice. The Big 4 Accountancy Firms also offer this service.

Establishing whether individuals or legal entities should be regarded as a PEP or their close associate is not straightforward and can present difficulties. Specialist Risk and Compliance search engines (e.g. Dow Jones or WorldCheck – subscriptions required) can often help identify potential PEPs, however close associates and family members can prove more difficult to identify and would often require further enhanced due diligence by experienced financial crime practitioners.

2. Why is combating money laundering and terrorist financing so important for FIs?

There are significant regulatory, reputational and commercial risks of onboarding or

financing individuals or companies involved or connected with laundering proceeds of crime or financing terrorism. These include:

- FIs can be subject to substantial regulatory fines and/or their operating license removed or suspended if they are found to be complicit in money laundering or terrorist financing or fail to notify authorities of suspicious activity.
- Directors and employees can receive custodial sentences if found to be facilitating money laundering or terrorist financing
- The FI can be subject to litigation and reputational damage for associating itself with such criminal activity including negative media attention resulting from fines.

Most of the jurisdictions in which BII invest have well developed AML/CFT laws but some countries across Africa and South Asia are still behind in having in place robust legislation and regulatory oversight compared to the US and Europe. The Financial Action Task Force (FATF), an intergovernmental organisation responsible for the setting of international standards and recommendations for ML/TF for countries monitors many jurisdictions for the effectiveness of implementation of these recommendations with findings published in Mutual Evaluation Reports (MERs). These provide FIs with a useful tool to assess the adequacy of the regulatory environment of the countries in which they operate to combat ML/TF, including reviewing the effectiveness of regulations and legal frameworks in place to address risks from ML/TF. This includes the ability to impose fines or prison sentences, the adequacy of a country's Financial Intelligence Unit (FIU) to receive and assess suspicious transactions reported by FIs, the extent a country shares relevant financial crime intelligence and the resources and technical competency in place to ensure effective oversight of regulated FIs.

3. Best practice management for FIs: The Risk-based approach

FIs should ensure they establish risk-based and proportionate policies, processes and resources to identify, assess and manage AML/CFT risks in line with local, national and applicable regulations and best practice. This includes conducting regular risk assessments to identify the level of controls an FI puts in place to manage and monitor AML/CFT risks. Outlined below is best practice guidance (and refer to FI BI Management Systems section for further guidance):

CLICK TO VIEW DIAGRAM

- AML/CFT Risk Assessment

  As a starting point, it is essential that AML/CFT policies and procedures are formulated following the undertaking of a firm-wide financial crime or AML/CFT risk assessment. The findings of the risk assessment should be shared with senior management to ensure that measures are developed and implemented to mitigate identified risks. Specific risk factors to consider when assessing AML/CFT risks include:

  - Jurisdictional risks, both in terms of location of operations (direct or through intermediaries) and customers;
  - Customer base – types/profile [e.g. personal customers (including unbanked/underbanked), High Net-Worth Individuals (HNWIs), Small & Medium sized Enterprises (SMEs), Corporates, Government/Public Institutions], geographies, size of customer base. This should also include identification of higher risk customer types (e.g. PEPs).
  - Distribution channels (e.g. face-to-face, digital/mobile)
  - Transaction types and currencies
  - Products and services offered by the FI (e.g. trade finance, wealth management, correspondent banking)

  AML/CFT policies and procedures should be informed by, and be proportionate to, the findings of the risk assessment, i.e. adopting a risk-based approach. The risk assessment should contain an assessment of the effectiveness of existing internal risk mitigation controls, documented and kept regularly updated (e.g. reviewed every 12 to 18 months).

- AML/CFT Policy

  Senior management should prepare a formal AML/CFT policy which includes, *inter*

alia, the following:

- A clear statement that the FI is committed to complying with relevant AML/CTF regulations (stating regulations and penalties for breaching them);
- Outline relevant national and international legislation and guidance on AML/CFT
- Outline responsibility for the policy and compliance team structure including nomination of a Money Laundering Reporting Officer (MLRO) or AML/CFT Compliance Officer
- Outline the ML stages and typical ML/TF red flags
- Outline a risk-based approach to AML/CFT and define prohibitions e.g. Shell Banks or not dealing with fictitious/anonymous entities/individuals
- A requirement that employees promptly report and escalate any knowledge or suspicion of money laundering and/or terrorist financing;
- A requirement to carry out appropriate customer due diligence (CDD) and "know your customer" (KYC) checks, including identification and verification of customers. Risk rating customers according to AML/CFT risks with enhanced CDD and more frequent reviews for identified higher risk customers (including PEPs), and outlining controls;
- Transaction Monitoring procedures to identify suspicious behaviour/activity in customer accounts (where applicable)
- Provision of regular training to employees;
- A clear statement that any breach will be considered an act of gross misconduct;
- Regular reporting requirements on effectiveness of implementation of the policy to Board / senior management and regulators.
- Record keeping provisions

Ideally, FIs should make a public statement or attestation of their AML/CFT policy on

their website. Useful guidance on the contents of the anti-money laundering policy and used by BII can be found in the Joint Money Laundering Steering Group's (JMLSG) anti-money laundering and counter-terrorist financing guidance.

BII's guidance on the structure of an AML/CFT Policy is provided below and the Resources section:

CLICK TO VIEW

- Appointment of a Money Laundering Reporting Officer or Compliance Officer

  Appointing a suitably qualified senior Manager or Director to oversee an FI's AML/CFT system and its management of money laundering risk is, in many jurisdictions, a regulatory requirement. It also helps demonstrate to investors that the issue is being seriously addressed and shows staff that it is an important concern and is likely to result in a more controlled and ordered approach to ML/TF risk. The duties of the officer are likely to include:

  - **Establishing and maintaining policies and procedures**
  - **Establishing and maintaining appropriate resource to manage AML/CFT risks**
  - **Overseeing compliance with the AML/CFT Policy** including reviewing audit/assurance reports (including KYC/CDD), suspicious transaction reports (STRs), regular reporting to senior management or a board committee on AML/CFT management information and maintaining the policy (including reflecting changes in AML/CFT regulations/international best practice).
  - **Reporting to the regulator:** If required, the Officer should report annually (or at whatever frequency stipulated) to the Regulator detailing compliance with AML/CTF rules and report to law enforcement relevant suspicious activity/STRs or to requests issued by law enforcement e.g. Production or Information Orders.
  - **Staff training:** The Officer should train or arrange training to ensure all staff understand the FI's AML/CFT policy & controls and their own responsibilities.

- **Record keeping:** The Officer should be responsible for ensuring that KYC files are kept for the required period of time stipulated by regulations and filing of STRs.

BII's guidance on the Job Description of an MLRO/CO is provided in the Resources section.

- Know Your Customer Checks and Customer Due Diligence

According to The FATF Recommendations (Recommendation 10), FIs should undertake customer due diligence in relation to a natural or legal person, persons acting on their behalf and beneficial owners in the following circumstances:

- When establishing a business relationship;
- When carrying out occasional transactions above a certain threshold (sometimes defined by country regulations e.g. for the EU, transactions over EUR 15,000)
- When there is a suspicion of money laundering or terrorist financing; or
- When there are doubts as to the authenticity or adequacy of previously obtained information.

The FI may not be able to deal with customers who are not able to satisfy the FI's due diligence requirements. FIs in developing markets should take into account financial inclusion principles when onboarding previously underbanked or unserved customers. For instance, FIs may apply simplified due diligence for low-risk financial products or consider alternative means of identification where a customer lacks standard verification documents. Guidance on simplified due diligence and alternative means of identification can be found in JMLSG Guidance: https://jmlsg.org.uk/guidance/current-guidance/ (referencing UK legislative requirements).

Customer due diligence measures for all customers

An FI should carry out the following checks for all new customers and ensure on-going regular checks throughout the course of the customer relationship (frequency of checks on existing customers should be aligned to the risk they present):

- Identification and verification of the customer's identity;
- Identification of the Beneficial Owners and Key Principles / Significant Controllers, and verification of their identity *(under the UK Money Laundering Regulations, a beneficial owner is an individual who ultimately owns >25% of a company's shares or voting rights, or who otherwise exercises control over a company or its management; this threshold will vary by jurisdiction and FIs may lower this percentage ownership to 10% or less where there is heightened risk of ML/TF e.g. in higher risk markets. Note BIIs threshold is >10%);*
- Understanding and, where applicable, obtaining information in relation to the nature of the business relationship or transaction; and
- Conducting ongoing due diligence on existing business relationships and the transactions undertaken through the duration of the relationship.

Additional customer due diligence measures for higher-risk customers

An FI should apply additional customer due diligence, or enhanced due diligence measures, to customers that present a higher financial crime risk. Higher risk customers include the following:

- PEPs and associates of PEPs;
- High-risk customers identified in accordance with the FI's own risk assessment e.g. operating in sectors prone to ML/TF e.g. money service businesses, cash-intensive businesses and or import/export and high value goods businesses (e.g. Jewellery);
- Customers established in a high-risk country (note alignment to FATF recommendations)
- Customers that provide false or stolen information or documentation or where the request for services does not make economic sense or is not considered bone-

fide.

- Customers with complex structures including the use accounts in offshore tax havens.

In addition to routine customer due diligence checks, FIs should, in relation to higher-risk customers, apply the following enhanced due diligence measures:

- Increase the frequency and nature of transaction monitoring to identify suspicious or unusual activity
- Obtain approval from senior management to establish, or continue the business relationship;
- Request additional information from the customer and regularly update and verify the identification of the customer and beneficial owner(s)
- Request additional information to establish source of wealth and source of funds; and,
- Request additional information on reasons and legal purpose of intended or performed transactions.

Information and documentation to be obtained for different types of customers

Useful guidance on information, documentation, and additional factors to consider for customer due diligence and enhanced due diligence in relation to different customer types can be found in FATF Recommendation 10 CDD and the JMLSG Guidance (referencing UK requirements)

- On-going monitoring & Transaction Monitoring

Ongoing monitoring is important to manage ML/TF risks. It is important for a FI to understand its customers' regular activities in accordance with their profile in order to identify abnormal activity or transactions that can be indicative of ML/TF and keep

KYC information up to date. Setting up transaction monitoring systems involves setting "rules" to allow the system to detect:

- unusual activity including detecting an excessive proportion of transactions that are just below the threshold for reporting purposes;
- abnormal transactional activity that deviates from norm e.g. a significant increase in transactional activity over a short time period, high value transactions or payments to parties that do not align with the customer's normal activity;
- changes to a customer's personal information e.g. name, address, and
- changes to a customer's trading activity e.g. goods, countries, currency.

The system will generate hits if it identifies such unusual activity for investigation by analysts in the FI to determine if they are true hits, which may involve requesting additional information or raising an internal suspicious transaction report. The analysis of these hits must be undertaken by suitably qualified staff.

Enhanced ongoing monitoring should be applied to higher-risk customers. In order to be able to meet this requirement, it is essential that a FI has an effective transaction monitoring system in place. The transaction monitoring system should be designed and operated proportionate to the FI's size and customer profile, which may require the automation of the monitoring process. Examples of specialist firms that offer this service include SAS, ComplyAdvantage, Actimize, BAeSystems NetReveal.

Useful guidance on ongoing monitoring can be found in Basel Paper – Sound Management of Risks Related to Money Laundering and Financing of Terrorism . JMLSG AML/CFT Guidance; International Finance Corporation (ICF) AML/CFT Guidance.

- Suspicious Transaction Reporting

Employees of the FI should be required to raise an internal report to the MLRO/Compliance Officer where they have any suspicion of ML/TF. They should

consider all internal reports and should report confirmed suspicions to the relevant authority (usually country Financial Intelligence Units which form part of the regulator or central bank).

Employees of the FI should refrain from releasing any information that might "tip off" a person that a report has been made. Several jurisdictions have made "tipping off" a criminal offence.

Suspicious transactions are most likely to be transactions that are inconsistent with a customer's known business or circumstances. Examples of what might constitute suspicious transactions are set out below.

- Counterparties with complicated corporate structures including offshore jurisdictions – particularly if the structure is not easily understood or its design is driven by secrecy
- Customers for whom verification of identity proves difficult and who are reluctant to provide identity details or other relevant documentation
- Customers who wish to use cheques drawn on an account other than their own or to have funds due to them paid into an account that is not their own
- Changes in settlement details at the last moment without satisfactory explanation
- Requests to transfer investments to apparently unrelated third parties
- Customers whose investment and lifestyle appear to be unrelated to their occupation
- Customers whose transactional activity is abnormal (see transaction monitoring above)

Where a disclosure is made before a transaction has occurred, the transaction should be halted pending the MLRO's/Compliance Officers consent to its proceeding. This may involve the MLRO /Compliance Officer submitting a Suspicious Activity Report to the Regulator with a view to informing them of the suspicion or requesting consent to proceed with a transaction, the latter is usually the case where they expect there to be proceeds of crime involved but will vary by jurisdiction.

Useful guidance on suspicious transactions reporting can be found in the JMLSG AML/CFT Guidance (referencing UK requirements)

- Record Keeping

  Although it will vary, most ML/TF Regulations will require an FI to retain CDD records for a certain length of time. This includes customer identification documents, customer risk assessments, relevant transaction data and STRs/SARs. For example, the UK Money Laundering Regulations require regulated FIs to retain CDD records for 5 years from the date the business relationship ends or from the date of an occasional transaction.

  Guidance on record keeping can be found in JMLSG Guidance: https://jmlsg.org.uk/guidance/current-guidance/ (referencing UK requirements)

- Training

  AML/CFT training should be given to all staff and relevant third parties to illustrate the importance of AML/CFT policies, procedures & systems to the firm. Training should ensure that staff are able to identify transactions which carry a heightened risk of ML/TF, including which indicators/red flags to look out for. Training should also make staff aware of their responsibilities under the FIs policy.

  Training is likely to involve initial education such as an introductory awareness course, which is followed up by updates and refresher courses. It may be given via a computer-based scheme, at a 'team' meeting or by an external professional brought in for the purpose.

  More detailed and tailored training on AML/CFT should be given to staff in financial crime departments responsible for the development and implementation of AML/CFT polices and processes in the firm. See FI BI Management Systems Section for further guidance.