BANK FOR INTERNATIONAL SETTLEMENTS

FSI Connect
Financial Stability Institute

AML and CFT in banking – Executive Summary

Jurisdictions outlaw money laundering (ML) to achieve three main objectives: (i) to curb criminality in general by making it difficult for criminals to reap the proceeds of their crimes; (ii) to protect the rights that are violated by crimes by aiding the seizure of illegally obtained funds; and (iii) to protect the integrity of the financial system more broadly. Terrorist financing (TF) is outlawed to deny terrorists access to funds and thus reduce the risk of attacks.

The exact legal definition of ML varies across jurisdictions, but it generally refers to acts that acquire, transfer or conceal proceeds of a certain criminal act. The underlying criminal act is referred to as "predicate crime". Most jurisdictional differences relate to what activity qualifies as a predicate crime. For example, some countries consider tax evasion as a predicate crime. In contrast, when dealing with TF[1], authorities are less concerned about the origins of funds and more with their intended use.

ML typically consists of three main phases:

1. Placement. Illegally obtained funds are introduced into the financial system, eg by depositing cash obtained from drug trafficking into a bank account.
2. Layering. The true origin of funds is concealed, eg by moving bank account balances, often across national borders.
3. Integration. The disguised funds are used for other legal purposes of investment or consumption.

Banks are particularly exposed to being abused for ML purposes. Private banking or asset management may be used for "layering" or "integration" purposes, while credit card or automated teller machine services can be used for the "placement" of illegal funds.

International payment services allow launderers to move money around the globe, creating layers that help conceal funds' origins. Correspondent banking is especially exposed, as it involves cross-border payments where the involved payer and payee are not necessarily known to all parties in the payment chain. Cryptoassets, being pseudonymous, create similar risks.

The abuse of financial intermediation can have repercussions that go beyond the individual transaction, as it threatens the stability of involved institutions and potentially the system at large. This demonstrates the need for preventative measures against ML, in addition to its prosecution as a crime.

International bodies and standard setters

Financial Action Task Force (FATF)

The FATF is an intergovernmental body that sets ML and TF prevention standards. The FATF focuses on three main areas:

- setting anti-money laundering (AML) and countering the financing of terrorism (CFT) standards through regularly updated FATF Recommendations; the current version, dating from 2012, was last updated in 2020

[1] In most other respects, dealing with TF is analogous to dealing with ML.

- evaluating progress through "mutual evaluations" of member countries by other member countries as to the compliance of jurisdictions' frameworks with the FATF Recommendations; this is supported by the 2013 Methodology for mutual evaluations
- identifying trends and engaging with high-risk, non-cooperative jurisdictions

The FATF Recommendations comprise a set of 40 specific recommendations that deal with the risk-based approach to supervision, provide relevant definitions, describe preventative measures that financial intermediaries should take and recommend powers national authorities would benefit from in the battle against ML and TF.

Basel Committee on Banking Supervision (BCBS)

The BCBS, the global standard setter for the prudential regulation of banks and a forum for cooperation on banking supervisory matters, incorporated the FATF Recommendations into its overall framework of banking supervision through guidelines[2] on the sound management of risks related to ML and TF, without modifying the content of the FATF Recommendations.

Other bodies

Other international bodies in the area of AML include the Egmont Group, an informal network of national financial intelligence units, and the Wolfsberg Group, a private sector initiative comprising 13 global banks.

AML and CFT in banking supervision

General principles

Banks' AML/CFT measures and related supervision should follow a risk-based approach. This entails a differentiation of risk classes and their separate management. Specifically, the risk-based approach requires the identification and assessment of the individual risk at hand, application of specific mitigation and monitoring measures, and documentation of the strategy taken and any major decisions made. Examples of suitable candidates for risk differentiation include:

- politically exposed persons (PEPs) – individuals who hold or have held important functions in the public or private sectors and may have been exposed to corruption. As corruption is a predicate crime, their wealth may be illicit, and hence transactions with PEPs warrant enhanced due diligence
- business areas that have a high cash turnover, eg casinos, parking garages and construction, warrant enhanced due diligence
- countries that are designated as non-cooperative by the FATF

Governance and organisation

The principal responsibility for a bank's ML/TF risk management lies with the board of directors. It is responsible for defining and overseeing a bank's AML/CFT policy and allocating operational responsibilities and resources under the "three lines of defence" model:

- The "first line of defence" lies with a bank's business units, eg its private banking or asset management divisions. These units are responsible for identifying, assessing and controlling ML/TF risks through the use of customer due diligence practices.
- The "second line of defence" primarily refers to the chief officer in charge of AML/CFT, the compliance function, as well as human resources and technology. These entities should be

[2] First issued in 2014, last updated in July 2020.

independent of business units, give independent advice to management and act as main contact point for the relevant authorities. Conflicts between the first and second lines of defence should be resolved at the highest level.

- The "third line of defence" refers to the independent internal audit function.

Banks' due diligence

Banks' due diligence refers to the collection and verification of client information at account opening and the monitoring of client transactions.

The overarching principle at account opening is "Know Your Customer" (KYC). This includes checking:

- the identity of an individual or a legal entity, including corporate officers or proxies (attorneys-in-fact), through appropriate documents (eg passports or certificates of incorporation)
- the financial and any criminal background of the customer, as well as the nature of a business or company
- how the bank relationship fits into the client's broader activities (eg salary account or operating account of a company)

The FATF has clarified that correspondent banks are not required to conduct due diligence on their respondent banks' clients, ie the ultimate payers or payees. Nevertheless, correspondent banks should assess the ML/TF risks associated with the correspondent banking relationship.[3]

Transaction monitoring is a particularly important aspect of banks' due diligence as it allows them to identify criminal activities and report those activities to the relevant authorities. The size of transactions and whether they are deemed suspicious govern escalation and reporting. With "large" transactions, reporting is triggered if certain, jurisdiction-specific thresholds are met. In terms of "suspicious" transactions, national AML regimes typically qualify such transactions as suspicious on the basis of the following patterns:

- The transactions do not "make economic sense", eg they have unrealistically high profits.
- "Structured" transactions are employed, ie multiple small transfers are used where one large transfer would have been more convenient but would have met an AML threshold.
- The transactions involve unusual withdrawals, especially if an account is closed and funds are withdrawn in cash.

Information management

To ensure a proper audit trail, foster sound supervisory reporting and, where necessary, support criminal prosecutions, banks should ensure that all information obtained through client and transaction due diligence is recorded and documented, including the inputting of transcripts into the bank's information technology systems. Recorded information should be retained for at least five years.

This Executive Summary and related tutorials are also available in FSI Connect, the online learning tool of the Bank for International Settlements.

[3] See the list of risk indicators in Annex 2 of the 2020 BCBS Guidelines.