Danske Bank

From Rules to Practice – How to Deal with AML and CFT Requirements

Danske Bank | 21 November 2019

Agenda

Thursday, November 21, 2019

1. **Opening Remarks**
2. **Latest AML/CFT Guidance for Institutions**
3. **Challenges to Institutions**
4. **Components of an Effective AML/CFT Compliance Program**
5. **Emerging Trends**
6. **Closing Remarks**

2 Latest AML/CFT Guidance for Institutions

Throughout 2019, a number of institutions have come under scrutiny for their alleged failure to enforce effective AML/CFT controls.

A **European Union**

On 24 July 2019, the EC published its "Communication from the commission to the European parliament towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework", which – alongside four reports – draws on 10 recent high-profile cases of alleged money laundering through EU banks to highlight what it identifies as the four main weaknesses of the current regime:

i. Ineffective compliance with AML/CFT legal requirements;
ii. Governance failures;
iii. The failure to mitigate high-risk business models; and
iv. Ineffective group AML/CFT policies.

The report calls for greater harmonization in supervision by national authorities, closer prudential supervision – particularly in cross-border situations – and more structured and systematic international cooperation with key non-EU authorities.

B **United Kingdom**

On 9 July 2019, the FCA published its "Anti-money Laundering Annual Report 2018/2019", revealing that the UK regulatory body has more than 60 ongoing AML investigations, some of which are being conducted on a dual-track basis, incorporating both criminal and regulatory investigations. The report shows that although the total number of financial penalties imposed by the FCA remains the same as the previous year, the value has increased significantly from £60.9MM to **£227.3MM**. When considering the fine levied against Standard Chartered Bank (£102MM), the FCA's actions emphasize the importance for banks to adopt an agile approach that goes beyond a box-ticking exercise.

C **United States**

On 22 July 2019, a working group comprising of the Board of Governors of the Federal Reserve System, the FDIC, the National Credit Union Administration, the OCC and the US Department of the Treasury's FinCEN issued its Joint Statement on Risk-Focused Bank Secrecy Act/Anti-money Laundering Supervision, which aims to provide greater clarity regarding the risk-focused approach used in BSA/AML examinations. The statement outlines common practices used to assess a bank's AML/CFT risk profile and highlights:

- That banks are encouraged to use a risk-based approach to manage customer relationships; and
- The regulators' view that a bank's board of directors provides guidance regarding acceptable risk exposure levels and corresponding policies, while management translates the board's goals, objectives, and risk limits into appropriate operating standards through policies, procedures, and practices.

Source: https://www.lexology.com/blog/2019/08/anti-money-laundering-latest-guidance-for-banks

3 Challenges to Institutions

Institutions are facing AML/CFT compliance challenges that can be typically attributed to faulty mitigation approaches. Institutions also face several challenges in managing risks involved in assessing the current AML/CFT status and identifying vulnerabilities. Disparate transactions and increasing complexities of fraud and cybercrimes compound the situation.

To address these challenges, institutions need to ensure data protection, detect fraud in time, and prioritize compliance with regulations (e.g., FATF).

The main challenges institutions face are:

Increased Governance: Institutions often find it difficult to manage cross-border and multi-jurisdictional AML/CFT compliance and CDD requirements. In addition, beneficial ownership and identifying remedial measures to address AML/CFT gaps uncovered by regulatory reviews pose their own set of challenges.

Lack of Skilled Personnel: Obtaining skilled resources with in-depth knowledge of AML/CFT can be challenging. Further issues include high onboarding timelines and costs, as well as attrition. Institutions also need to ensure that they are investing sufficient time and effort in keeping personnel up-to-date with changing regulatory requirements.

Compliance Processes and Technology: In order to comply with AML/CFT requirements, institutions must put in place a multiplicity of processes and technology solutions that will, for example, consolidate KYC data and systems in a single repository. There is also a need to create infrastructure for cross-channel detection of suspicious activities, improve data quality, and standardize data to enable centralized analysis of financial crimes.

4 Components of an Effective AML/CFT Compliance Program

An AML/CFT Compliance Program is a methodology that defines how a company monitors accounts and detects and reports financial crimes to relevant authorities. An institution's AML/CFT Compliance Program should be able to reasonably detect money laundering, tax evasion, fraud, and terrorist financing through its accounts. It should have systems to immediately report money laundering activity to relevant authorities and also evaluate its client's risk profile.

A AML/CFT Fundamentals

- ***Written Policies***: State them clearly and have it written out for all (executives, staff, and regulators).
- ***Compliance Officer***: Designate one individual to "own" the system and ensure that processes are followed and updated, reports are filed, training is correct, and that the system is running smoothly.
- ***Training***: Employees need to understand the institution's policies and procedures, legal requirements, techniques used by money launderers, checks they should perform, and how to report suspicious activity. To ensure the program is up-to-date, perform periodic refreshers.
- ***Review***: Have an independent expert, such as a third-party, review your program on a periodic basis.

B AML /CFT Risk Management

- ***Risk Assessment***: Risk assessments give a full understanding of the different tiers of risks a customer presents and how to mitigate them, and is based on a scoring model. This scoring model must consider risk factors such as geographical location, PEPs, UBOs, and outcome of the required KYC due diligence process, i.e. CDD and EDD. Determining risk assessments is about creating policies and procedures that are dynamic, defendable, and adaptable. Regulators are trending toward a more risk-based approach.

C AML/CFT Red Flags

Examples of unusual activities:

- Large cash transactions
- Large amounts of transactions (layering)
- Spikes in activity or amounts
- Transactions connected with cash-heavy businesses

These activities are noticeable in the initial due diligence process or through ongoing monitoring. During onboarding, a baseline for normal activities should be established (e.g., by SoF, account type).

D AML/CFT Screening

The best way to mitigate risk is to detect and manage problematic accounts before they become a risk. Performing a comprehensive identity verification check reduces risk from fraud, risk of breaking compliance rules, and risk from dealing with money obtained from illicit activities.

By blocking access to those that want to bypass your safeguards in the first place, your prevention systems will be more robust and secure.

E AML/CFT Monitoring

Monitoring refers to the analysis of continual, ongoing activities to ensure activities remain in compliance.

Examples of activities to keep track of:

- Exceeding thresholds
- Transactions with no business purpose
- Change of status
- Recording of communications
- Surveillance of employees
- Watchlists
- Market trends
- Trade data

F AML/CFT Compliance Technology

Technologies that add to, or improve, existing processes are attracting the most attention. Identify proven technologies, not just ones having potential (e.g., Blockchain).

Automation will not eliminate the need for human evaluation and judgement, especially in investigations. However, automation streamlines the process, reduces regulatory risk, and avoids unnecessary charges for people handling repetitive tasks that are better suited to computers.

Sources: https://sumsub.com/knowledgebase/aml-compliance-progam/; https://www.trulioo.com/blog/aml-compliance/

5 Emerging Trends

A new pattern is emerging wherein principle-based AML/CFT systems are replacing inflexible rules-based solutions. Some emerging trends in AML/CFT compliance are:

Focus on Digital Payment-Related Issues: Regulatory focus is currently centered on containing money laundering risks associated with new payment methods, such as mobile wallets, e-payments, and e-money issuers.

Use of Third-Party Utilities: Third-party services such as the shared services utility model for KYC compliance, managed services for transaction monitoring, and browser-based delivery of commercial watchlists are currently being explored in several institutions.

Adoption of Enterprise-Level Approaches: Enterprise-wide case management for an overall view of risks at the enterprise level, and effective centralized control is becoming the norm. Risk-based approaches are replacing traditional rule-based approaches.

Adoption of Analytics: Institutions are adopting analytics for their AML/CFT initiatives in areas such as: fraud detection, screening, detection of rogue activities, similarity detection, trending analysis, anomaly detection, and trusted pair identification.

What about the role of machine learning?

- Aided by the significant developments in data science, machine learning is revolutionizing the way financial ecosystems work. Machine learning is especially promising in the area of detecting hidden patterns and suspicious money laundering activities.
- Machine learning assists in identifying money laundering typologies, strange and suspicious transactions, behavioural transitions in customers, transactions of customers belonging to the same geography, age, groups, and other identities, and helps reduce false positives.