

Anti-Money Laundering: Challenges and Trends

Abstract

The inadvertent use of the banking system for money laundering activities is a key challenge facing the financial services industry. In response, regulatory authorities have introduced anti-money laundering (AML) regulations to detect and prevent such activities. Complying with these regulations requires banks and financial institutions to implement an effective compliance system, along with appropriate tools and systems. This, in turn, requires companies to build an effective business case for the right compliance system equipped with requisite capabilities and latest technology tools.

This paper discusses the challenges before banks and financial institutions, prevailing industry trends, and how emerging technologies can be used to monitor transactions to identify suspicious activities.

Some Challenges that Exist Today

Banks and financial institutions are facing some serious AML compliance challenges that can be typically attributed to faulty mitigation approaches. Firms that fail to prevent laundering tend to pay a heavy price in the form of declining revenues, customer dissatisfaction, huge penalties, loss of reputation, and fall in stock prices.

To comply with AML regulations, banks around the world use various technology-based products and solutions.

The Financial Action Task Force (FATF), an inter-governmental body with 37 members the world over, has framed a set of regulations that is recognized as an international framework of AML standards. These AML regulations help detect, report, and prevent suspicious activities at financial institutions.

Banks face several challenges in managing risks involved in assessing the current AML status and identifying vulnerabilities. Disparate transactions and increasing complexities of fraud and cybercrimes compound the situation. To address these challenges, banks need to ensure data protection, detect fraud in time, and prioritize compliance with the FATF regulations.

Here are the other challenges banks face:

Increased governance: Banks and financial institutions can find it difficult to manage cross-border and multi-jurisdictional AML-compliance requirements and ever-growing customer due diligence requirements. Identifying beneficial ownership and initiating remedial measures to address AML gaps uncovered by regulatory reviews also come with their own set of challenges.

Lack of skilled personnel: Getting skilled resources with in-depth knowledge of AML can be a challenge. Other issues include high on-boarding timelines and costs, and attrition. Organizations also need to invest considerable time and effort in keeping personnel abreast with changing regulatory requirements.

Complicated processes and technology: AML compliance requires banks to put in place a multiplicity of processes and technology solutions that will consolidate KYC data and systems in a single repository. They also need to create infrastructure for cross-channel detection of suspicious activities, improve data quality, and standardize data to enable centralized analysis of fraud and financial crimes.

The risk level assigned during on-boarding varies according to the transactions undertaken by the customer. This means that banks have to assess the risks dynamically for each customer, and change risk levels accordingly, to prevent false positives. This necessitates continual transaction monitoring for each customer, which is a mammoth task.

Emerging Trends in the AML Space

A new paradigm is emerging wherein principle-based AML systems grounded in scientific disciplines are replacing inflexible rules-based solutions. Some emerging trends in AML compliance are:

Focus on digital payment-related issues: Regulatory focus is currently centered on containing money-laundering risks associated with new payment methods like mobile wallets, e-payments, and e-money issuers. In addition, top priority is being accorded to combating cybercrime and curbing potential money-laundering risks associated with virtual currencies.

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 watch lists are being leveraged by several banks. Financial institutions are using the expertise of third-party providers for KYC verification and due diligence, and to spot new AML risks and violation methods.

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. Banks are also implementing AML or fraud platform convergence capable of detecting both

fraud and money-laundering activities to derive operational synergies. Risk-based approaches are replacing traditional rule-based approaches.

Adoption of analytics: Banks are adopting analytics for their AML initiatives. Some areas where analytics can be used successfully include:

- **Fraud detection:** Advanced filtering technologies and analytics for real-time fraud detection and generation of alerts based on changes in behavior patterns are gaining ground. Banks are also using high-tech linkage analysis (network visualization) to detect suspicious activities and track money trails. They are using cross-channel detection support to get an integrated view of suspicious activities across all payment types and anti-stripping technology to detect masking or manipulation of wire transfer data.
- **Screening:** Banks are tapping social media as an additional source of information to validate customer identity, identify politically exposed persons (PEP), and obtain default information for account reviews of a customer. Banks are leveraging social media analytics to support their enhanced due diligence (EDD) process, which includes negative media screening efforts for discovery of litigations, adverse orders, and other potential risks. Banks are also using software for sanctions screening, which results in benefits such as reduced timelines for enhanced due diligence; faster and informed decision making; quicker identification of key risks associated with companies, management teams, and other affiliates; and faster processing of transactions and monitoring of alerts.
- **Detection of rogue activities:** Banks are using analytics to detect anomalies and identify patterns indicative of laundering, and detect and prevent suspicious activities in real time. High speed streaming and computing to handle transaction data in all formats, parallel processing of transaction data and data from other channels, and high-speed alert generation and processing are other trends that are catching up.

- Linkage detection: Banks and financial institutions are using analytics to detect entity-level linkages, and study the behavior of different linked accounts colluding for a laundering activity. Some of the linkages that can be tracked include:
 - Linked customer: To identify IDs owned by the same customer across lines of business.
 - Linked accounts: To track customers having multiple accounts under different names.
 - Linked transactions: To track transactions linked to a closed group of entities and performed with a clear intention of routing money to destination accounts
 - Linked access: To track transactions happening through common cyber infrastructure.
- Similarity detection: This can be used to analyze data at fixed intervals in order to find similarities in current and past financial crimes, which helps eliminate redundant investigation and create stronger cases.
- Trending analysis: This technique can help identify behavioral trends using cognitive computing of non-parametric statistics. With this, banks can identify behaviors and bad actors associated with money-laundering activities.
- Anomaly detection: This can help detect and study unusual behavior of a single actor.
- Trusted pair identification: This technique can help banks identify and ignore trusted pairs of parties through link analyses patterns, thereby reducing false positives.

The Role of Machine Learning

Aided by rapid developments in data science, machine learning, with its ability to help construct algorithms for predictive data analysis, is revolutionizing the way financial ecosystems work. Machine learning holds great promise for the banking system, especially in the area of detecting hidden patterns and suspicious money-laundering activities.

Machine learning helps identify money-laundering typologies, strange and suspicious transactions, behavioral transitions in customers, transactions of customers belonging to same geography, age, groups and other identities; and helps reduce false positives. It also helps analyze similar transactions for focal entities and correlate alerts that were flagged as suspicious in regulatory reports.

Conclusion

Money launderers will always find newer ways to use banks for illegal activities. The timely detection of laundering activities is the most challenging aspect in the implementation of an efficient AML program. Several innovative technology-based tools and products are currently available to detect, track, and prevent money laundering. Though these technology tools will not completely eliminate money laundering, they will bring it under control to a large extent, and financial institutions should proactively look at adopting these sooner than later.

About The Author

Vani Muppayyanamath

Vani Muppayyanamath is a Domain Consultant with the Banking and Financial Services (BFS) business unit of Tata Consultancy Services (TCS). She has over seven years of experience in the implementation of financial solutions such as the Oracle Financial Services Analytical Applications (OFSAA) — Financial Crime and Compliance Management (FCCM), with special focus on anti-money laundering, fraud and crime detection, and regulatory compliance.

Contact

Visit the [Banking & Financial Services](#) page on www.tcs.com

Email: bfs.marketing@tcs.com

Blog: [Drive Governance](#)

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w

Feedburner: <http://feeds2.feedburner.com/tcswhitepapers>

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com