FRAML and beyond – fighting crime, the integrated way



A collaborative article by Chartis and NICE Actimize

Why FRAML?

An integrated initiative

Use of the term 'FRAML' – to denote a combination of fraud and anti-money laundering (AML) processes and systems – signifies a growing trend among financial institutions, a recognition of the overlap between fraud and money laundering schemes (see Figure 1). It also emphasizes how employing a unified strategy to combat these crimes can be effective.

Figure 1: The increasing convergence of fraud and AML
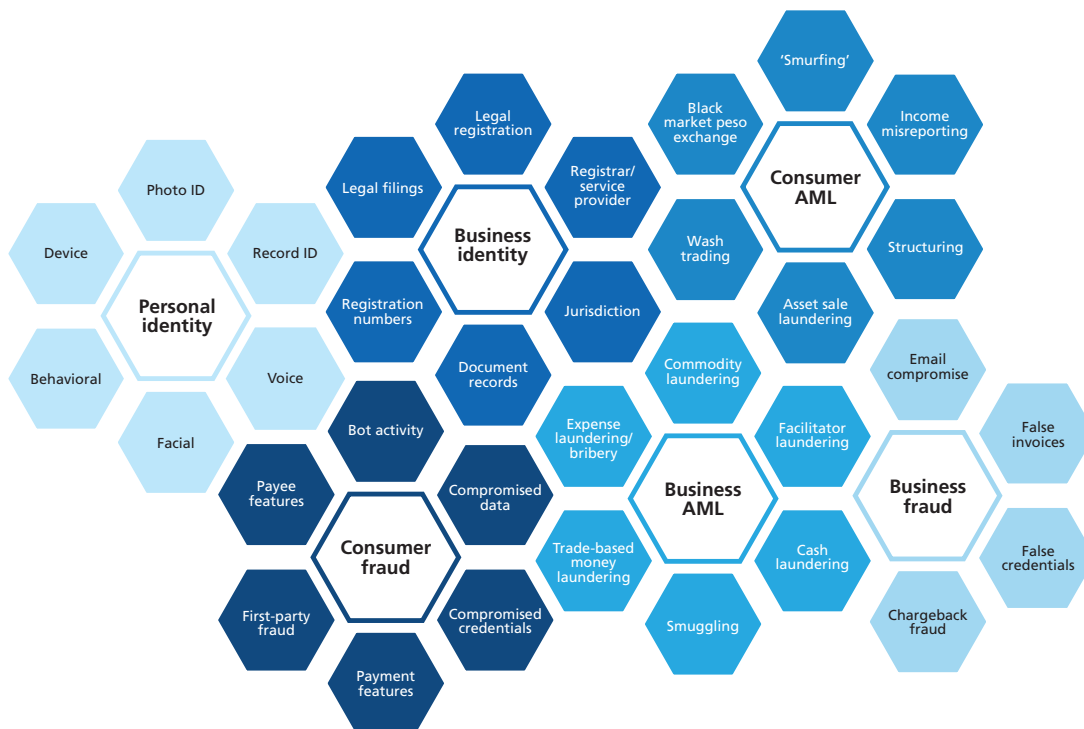
Source: Chartis Research

Defining FRAML

In criminal terms, fraud and money laundering are closely related: fraudulent activity can be a red flag for potential money laundering. The two risk types also share similar detection and mitigation strategies, including:

- Identifying suspicious actions.

- Escalating risks.

- Taking steps to stop criminal activity (such as blocking accounts).

- Communicating effectively within and between financial crime compliance and fraud prevention teams.

While organizations traditionally treated fraud prevention and AML separately, as an issue of security and an area of compliance respectively, criminals don't see a difference. This has led to a growing trend among many firms: combining these teams under a single umbrella, 'FRAML,' to engender a more holistic approach to combatting financial crime.

Indeed, as financial institutions develop systems that are more connected, they may move beyond FRAML and adopt a more wide-reaching approach.

Fraud prevention and AML teams typically share key objectives, including:

- Shielding customers and protecting organizations from the impacts of financial crime.

- Staying compliant with regulations.

And for financial institutions, developing an integrated platform can bring several key benefits:

- **A unified view of risk**. A FRAML approach can break down information silos, giving both fraud and AML teams a complete picture of potential threats. By sharing data on individuals and entities, firms can identify risks earlier and make better decisions faster.

- **Cost savings**. By combining teams, firms can create operational efficiencies. Resources can be shared and staff can be redeployed between fraud and AML duties as required, improving flexibility and collaboration within the organization.

- **A centralized approach**. FRAML enables firms to develop a single, coordinated anti-FinCrime effort. This allows for smoother information flow, faster response times and better use of existing expertise.

- **Scalability and efficiency**. By employing FRAML solutions in the cloud, firms can eliminate the need for expensive on-premise infrastructure. They can collect and analyze data from diverse sources, automate tasks and provide valuable insights to optimize their allocation of resources.

A stepping stone to holistic risk management

The idea of merging traditionally separate fraud and AML teams is gaining significant traction. Nevertheless, the term 'FRAML' may be a temporary label. Combining these workflows can clearly offer substantial benefits, but many firms are considering an even bigger picture.

For many, the first step is incorporating the entire Know Your Customer (KYC) process into their anti-FinCrime approach. But their ultimate objective is to obtain a real-time view of customer risk, which would include such dynamic factors as customer and transaction behavior, alongside more traditional, static KYC information (such as employment data, personal details and ID documents).

In this context, FRAML becomes a stepping stone toward a more comprehensive risk management strategy that focuses on the goal of real-time risk assessment.

Effective FRAML – and how to achieve it

Machine learning – the powerhouse of real-time fraud detection and prevention

By enabling real-time analysis, machine learning (ML) tools have become a transformative element of fraud detection. Many firms also use ML extensively to automate key tasks within FRAML compliance, such as:

- **Automated customer due diligence (CDD)**. Traditionally, analysts spent hours sifting through data to identify customer risks. ML can analyze massive datasets in seconds, saving time and resources for compliance teams.

- **Streamlined monitoring and reporting**. ML tools can continuously monitor customer activity and flag suspicious behavior so that analysts can investigate potential crimes and report them to the authorities. They can also automate tasks such as transaction monitoring and dashboard generation, boosting operational efficiency.

- **Enhanced internal controls**. ML can also evaluate internal controls, pinpointing weaknesses in a system. While advanced tools are still emerging, they could revolutionize FRAML compliance – emphasizing the importance of early adoption by vendors and financial institutions.

Unlocking efficiency gains: the single-platform advantage

A single FinCrime platform plays a vital role in a complex and ever-evolving landscape of threats. By unifying disparate systems and workflows for fraud and AML activities, these platforms offer significant advantages. They can streamline investigations, enhance collaboration and provide a holistic view of risk, ultimately empowering organizations to combat financial crime more effectively and efficiently.

A single FRAML platform provides the following key functionalities:

- **Streamlining workflows by eliminating siloed data**. A single platform centralizes data, eliminating the need to search for information across multiple sources. This saves time and reduces the risk of errors.

- **Enhancing collaboration** by sharing information in real time, improving visibility and breaking down departmental barriers.

- **Enabling faster decisions** by identifying risk faster, improving data analysis and reducing the time taken for investigations and reviews.

Beyond human limits: generative AI as a tool for financial crime compliance

Generative artificial intelligence (GenAI) is a powerful tool that's revolutionizing the way financial institutions fight fraud and money laundering. By leveraging its capabilities, firms can build a more robust FRAML defense and protect their customers and members. However, it is important to remember that GenAI is a tool – human expertise remains crucial for interpreting results and making final decisions. And as with any AI technology, ensuring fairness and avoiding bias in generative models is essential.

A FRAML platform leveraging GenAI provides the following key capabilities:

- **Automation of repetitive tasks** such as data analysis, report generation and alert triage. This can free up analysts to focus on more strategic work and complex cases.

- **Faster, more compliant reporting**. Suspicious activity reports (SARs) can be generated automatically based on investigation data. This speeds up the reporting process and ensures that reports are accurate and compliant with all applicable regulations.

- **More efficient analysts**. By automating human-led, repetitive tasks and providing insights, GenAI can enable analysts to investigate cases faster, prioritize alerts more effectively, and make better, more informed decisions.

NICE Actimize – a FRAML category leader

NICE Actimize's Xceed AI FRAML is a built-for-purpose fraud and AML solution designed to help financial institutions identify and prevent financial crime in real time. It has achieved category leader status for FRAML solutions largely because it offers in-depth analysis capabilities across all stages of the analytics lifecycle, from data management to discovery to the deployment of AI into production. By monitoring individuals and entities within a FinCrime framework, using data that is constantly improving, users can make more informed decisions throughout the whole customer lifecycle.

The Xceed FRAML solution is a self-learning financial crime and compliance platform designed around the unified Fraud and AML evidence lake. It aims for quick time-to-value to prevent fraud and detect money laundering in the mid-tier to small and mid-size business (SMB) markets. Xceed AI FRAML provides AI as a service (AIaaS)[1] with classes of algorithms that include Bayesian network probabilistic graphical fraud detection and GenAI purpose-tuned large language models (LLMs).

Xceed's new assistant uses the power of GenAI to target efficiency gains in mid-market banks and credit unions in the fight against financial crime. By using GenAI, Xceed FraudDESK CoPilot automates the repetitive tasks involved in investigating and reporting financial crime, focusing on alert triage, prioritization and case narration. Fraud analysts can focus on what truly matters – fighting financial crime – making their time more meaningful.

Key functions include:

- Real-time transaction monitoring, fraud detection and fraud intervention.

- Detection of intricate cross-channel fraud schemes.

- Automated and streamlined filing of SARs.

The solution's real-time transaction monitoring, fraud detection and fraud intervention tools employ a unique AI-first approach using NICE Actimize's patented risk engine. Xceed AI FRAML creates real-time profiles of customers' risk based on their live transaction and behavioral data. It also enables financial institutions to tailor their fraud prevention strategies to individual customers in real time. This analysis allows for faster and more accurate detection and prevention of fraud.

The solution also detects cross-channel fraud schemes via omnichannel monitoring. Xceed is designed to monitor financial risk and fraud across various channels (including wire and automated clearing house (ACH) transfers, digital payments such as person-to-person (P2P), Zelle and Venmo, and core banking systems), giving financial institutions a comprehensive view of customer activity. Xceed's patented self-learning algorithms are trained to monitor vast amounts of data across channels, with the aim of identifying potential fraud attempts across different platforms.

Xceed's ability to reduce false positives is another strong aspect of the solution. With its self-learning capabilities and real-time anomaly detection, the system can learn and adapt to new fraud tactics and ever-evolving customer behaviors. The solution establishes a behavioral baseline for each customer's expected values (such as the quantity and monthly value of their incoming and outgoing transactions). Over time this self-adjusts as the algorithms learn behavioral patterns. As time passes, each metric becomes more precise, enabling the system to filter out more false positives and negatives, and ensuring that Xceed remains effective as the fraud landscape changes.

Integrated case management and interactive dashboarding capabilities are particularly strong in Xceed AI FRAML and all compliance and risk investigations can be located and managed from a centralized location. Heatmapping functionality gives analysts a full transaction drill-down, providing quick access and intuitive understanding of the critical details of investigations. Link analysis offers further visualization of money flows across accounts, and parties can view all associated risk factors. These tools enable investigators to rapidly identify relationships and links between potentially suspicious activities. Other tasks, such as KYC checks and SAR filings, are streamlined and automated. Xceed allows for quick and intuitive access to all pertinent information on a single platform, enabling analysts and investigators to become more efficient and make better-informed decisions.

---

[1] A cloud-based service model that allows individuals and businesses to access and leverage AI functions without having to build and maintain their own AI infrastructure in-house.