HAWK:AI

WHITEPAPER

ELECTRONIC TRANSACTIONS ASSOCIATION WEBINAR RECAP

www.hawk.ai

HAWK:AI's mission is to help financial institutions detect financial crime more effectively and efficiently using AI to enhance rules and find anomalies.

FRAML: BENEFITS AND CHALLENGES OF A HOLISTIC RISK APPROACH

FRAML, the convergence of Fraud and Anti-Money Laundering (AML), is changing the compliance and risk management landscape for financial institutions. Just like any other emerging trend, FRAML brings potential upside and obstacles. In a webinar hosted by the Electronic Transactions Association (ETA) and sponsored by HAWK AI, a panel of Fraud & AML experts discussed launching and scaling FRAML operations, sharing information between teams, and the challenges and benefits inherent in a combined Fraud and AML approach.

The Panelists
Moderator: Caroline Hometh – Managing Partner, RPY
Wolfgang Berner, Co-founder, & CTO/CPO, Hawk AI
Christopher Mascaro, Chief Risk Officer, NAB
Armen Khachadourian, Executive Consultant, Global Vision Group

WHAT IS FRAML?

The panel began by defining FRAML itself. FRAML is a comprehensive approach that combines fraud detection with anti-money laundering (AML) measures. It recognizes that fraud is frequently a precursor or predicate offense to money laundering. By integrating fraud detection and AML techniques, FRAML aims to identify and prevent illicit activities across the board. This unified framework allows financial institutions to enhance their risk management capabilities, uncover interconnected criminal schemes, and mitigate the potential financial, reputational, and legal risks associated with fraudulent transactions and money laundering.

"If you know how the funds are initially obtained, you can better track them throughout the system."

Christopher Mascaro
Chief Risk Officer, NAB

"When you're looking at things holistically, you can do a lot more," said Christopher Mascaro. "If you know how the funds are initially obtained, you can better track them throughout the system."

Fraud and anti-money laundering functions within financial institutions have traditionally operated as separate entities, each with its own set of responsibilities and objectives. However, these two areas can greatly benefit from cooperation and information sharing. By working in tandem, these functions can gain a more comprehensive understanding of both fraud and financial crime. Patterns and trends that may indicate potential fraud or money laundering schemes can be identified more quickly and effectively. The two teams can streamline investigation processes, combining the expertise of both functions.

"Fraud needs immediate attention. If you don't get it, you are going to lose money very fast."

Armen Khachadourian
Executive Consultant,
Global Vision Group

"There are two separate organizations, and the reason for that is the talent and the resources it takes to manage it is very different," said Armen Khachadourian. "Fraud needs immediate attention. If you don't get it, you are going to lose money very fast. AML is compliance [and retrospective]. It is important that the information is shared between the two organizations rather than being siloed."

Wolfgang Berner gave an example of an instance where a client benefited from a FRAML approach. A banking client caught an eBay scam where someone was pretending to sell iPhones. The person aggregated the funds in one account, which raised a red flag for fraud. Once the funds were aggregated, they were funneled out to the next account and moved to another country, the first step in a money laundering scheme. Within days, the client saw fraud evolve into money laundering, and their investigations benefited from this additional context.

REGULATORY PRESSURE ON FINANCIAL INSTITUTIONS

In recent years, there has been a noticeable surge in regulatory pressure on financial institutions to intensify their efforts in combating financial crime. Regulators are increasing scrutiny of the monitoring, detection, and reporting capabilities of financial institutions. Financial institutions continue to face mounting penalties for not adequately monitoring transactions for financial crime. It is up to financial institutions to strengthen their detection efforts so they can sustain this regulatory pressure.

In contrast to other regions where payments processors are regulated directly, in the United States, payment processors are usually regulated indirectly through sponsor banks. Due to the complex nature of the payments ecosystem, these sponsor banks typically assume the responsibility of overseeing and ensuring compliance for the payments companies they work with. With regulatory pressure on their sponsor banks increasing, payments companies will likely see expectations for monitoring capabilities to trickle down to them.

TRANSACTION DIGITIZATION AND MARKET PRESSURE ON FINANCIAL INSTITUTIONS

As transactions increasingly shift towards digital platforms, the methods of perpetrating fraud have also adapted to exploit this digital landscape. Khachadourian gave the notable example of the rise of fraud occurring through prepaid cards. These fraudsters use prepaid cards to make illegal purchases, accept fraudulent payments, or arrange payment to facilitate larger scams. Financial institutions now face immense market pressure to keep pace with sophisticated fraud and financial crime methodologies. To combat these challenges, fraud and AML teams need to collaborate effectively and break down information silos.

INFORMATION SILOS BETWEEN FRAUD AND AML

Fraud and AML are often different teams with different processes. Because fraud is real-time and AML is retrospective, it sometimes makes sense for these two teams to remain separate. However, information silos between the teams can hinder their ability to effectively detect fraud and financial crime. These silos occur when there is limited communication, collaboration, and information sharing between the two teams, resulting in fragmented insights, and missed opportunities to detect interconnected fraudulent and money laundering activities. To bridge these silos, it is crucial for financial institutions to foster a culture of collaboration and establish effective channels of communication.

There are many ways to bridge the information silos. Encouraging regular meetings, joint training sessions, and cross-functional projects can promote knowledge sharing and facilitate a better understanding of each team's expertise and perspectives. Implementing integrated technology platforms and data-sharing systems can further break down information barriers, enabling real-time access to relevant information and analysis for both Fraud and AML teams.
By bridging these information silos, financial institutions can improve their overall effectiveness in detecting fraud and money laundering, leading to better protection for both the institution and its customers.

In addition to encouraging collaboration and communication between Fraud and AML teams, financial institutions can train their entire organizations on Fraud and AML. Mascaro pointed to North American Bancard's customer care team as an example. This team speaks regularly with merchants, agents, and their customers. Members of the customer care team will often notice suspicious behavior from a merchant, such as not knowing what they sell. The customer care team will escalate those hints to the fraud team to investigate. This is just one instance of how sharing Fraud and AML information can benefit financial institutions.

DEGREES OF FRAML INTEGRATION

As a solution provider, Hawk AI has seen varying degrees of FRAML integration, ranging from strict separation to full integration. Large, established financial institutions tend to have larger, fully separate teams. On the other hand, smaller and/or younger financial institutions often fully combine Fraud and AML teams and operations. The primary challenge of full integration is data orchestration between a patchwork of disparate systems. Many of these systems have been in place for years and are difficult to replace or rework for FRAML operations. Regardless of the degree of FRAML integration, the important elements for a holistic risk approach are appropriate reporting structure, constant communication, tooling support, and organization-wide training.

> Regardless of the degree of FRAML integration, the important elements for a holistic risk approach are appropriate reporting structure, constant communication, tooling support, and organization-wide training.

USING AI TO DETECT SUSPICIOUS FINANCIAL ACTIVITY

In whatever form they integrate, Fraud and AML teams can both use powerful AI and machine learning technology to detect suspicious activity. For example, anomaly detection models look for deviations from normal customer transactional behavior, comparing these behaviors to the customer's own history and peer behavior. Investigators can also use AI to reduce false positive alerts, focusing human investigators attention on true positive cases. The AI models can do this in real-time, preventing friction in customer experience.

"False positive or not, you don't want your fraud monitoring system to be a sales prevention task force," said Khachadourian. "You want sales to take place, you just don't want to take any fraudulent transactions."

> *"It can be as a response to what you have found from anomaly detection, you see a certain pattern, and then you search for it specifically."*
>
> **Wolfgang Berner**
> Co-founder, & CTO/CPO, Hawk AI

In addition to reducing false positives and detecting anomalies, we can also train AI models to look for specific typologies and behaviors. "It can be as a response to what you have found from anomaly detection," said Berner. "You see a certain pattern, and then you search for it specifically." AI models can also be trained to identify already well-known patterns, or even new patterns that emerge as fraud or money laundering threats.

The core difference between using this technology for Fraud and for AML is timing. As mentioned already, fraud detection occurs in real-time, while AML is often retrospective. Most financial institutions simply process too many transactions for human investigators to monitor in real time. "We're talking milliseconds," said Mascaro. "10, 20, 50, 100 milliseconds. Humans can't make decisions that quickly." Regardless of the timing of the monitoring, FIs can leverage AI technology to process billions of transactions, something that's just not possible for human investigators.

COMBINING TECH POWER WITH HUMAN POWER

From Mascaro's point of view, AI technology won't replace humans in Fraud or AML. However, he did predict that more financial institutions will adopt AI to serve as a human aid. AI can act as a "virtual teammate," reviewing transaction data in volumes that no human team, regardless of size, can review. Human operators can also use their risk and compliance expertise to optimize the results of AI models. Whatever happens in the future, Fraud and AML teams alike can reap huge benefits by effectively combining their human resources with effective technology resources.

HAWK:AI

HAWK:AI GmbH
Friedenstrasse 22B/i3
81671 München
Deutschland

HAWK:AI USA Inc
230 Park Ave., Floors 3 & 4
New York, NY 10169

+49 89 2555 2420
info@hawk.ai

Twitter: @hawkAI
LinkedIn: @HawkAI

www.hawk.ai