CEP Magazine - March 2024

Nick Parfitt (nick.parfitt@feedzai.com) is an anti-money laundering subject matter expert at Feedzai in London, England, U.K.

AML tactics are failing: Here's how we turn it around

By Nick Parfitt

According to the United Nations, $2 trillion is laundered annually, with only 1% of these illicit funds intercepted.[1] The scale of the problem is immense, and anti-money laundering (AML) compliance efforts cost financial institutions a hefty $213.9 billion globally.[2] So, why are AML strategies not working as effectively as they should be?

Alongside the existing issues with AML tools, criminals are becoming more sophisticated, using novel technologies to fool legacy systems and leaving compliance teams unable to keep up.

A fundamental refresh of how we approach AML is required to equip professionals with the right support to tackle these issues effectively—and automation has a huge part to play in this.

The shifting money laundering landscape

Nearly half (46%) of AML compliance professionals believe increasingly sophisticated money laundering techniques are one of the biggest threats their businesses face.[3] The threat from generative artificial intelligence (AI) and linked technology is now viewed as the top challenge for AML professionals, overtaking regulation, cryptocurrency, and blockchain—the top threats cited in 2022.

Generative AI is just the latest technological advancement that has been added to a fraudster's armory. Bad actors are fooling existing AML processing systems, which are often unable to detect illicit activity or encrypted data. Financial criminals continuously devise new and innovative methods to defraud their targets, underscoring the crucial need for constantly updated AML capabilities and strategies to outpace their ingenuity.

AML's current shortfall against financial criminals

Before understanding how we develop AML tactics, we must look at why they're currently failing. According to Deloitte research, compliance failures have led to banks paying steep penalties, with the total figure in fines reaching $5 billion in 2022 globally, up 50% from the previous year.[4]

A fundamental failure compliance teams must grapple with is ineffective transaction monitoring. Current monitoring alerts are outdated and can wrongly flag a Suspicious Activity Report (SAR). However, it's estimated that 95% of system-generated alerts are considered false positives.[5] Due to regulatory requirements, compliance teams must investigate every suspicious alert or face significant fines, but with such high alert volumes, it's becoming increasingly challenging to keep up.

Cryptocurrency also presents a challenge for compliance professionals with new avenues for criminals to launder the proceeds of illicit activity. In 2022, illicit addresses sent nearly $23.8 billion worth of cryptocurrency—a 68% increase from 2021.[6]

Over half (53%) of compliance professionals report money that laundering activities are broadly related to crypto transactions.[7] Yet, our research revealed that 40% of compliance professionals admit that crypto monitoring was the area of their AML program that is the least successful or is still developing.

Cryptocurrency's complex transaction patterns are a concern for compliance teams. Transactions can involve multiple wallets and exchanges, making it difficult for banks to identify the true source and destination of funds. Cryptocurrencies also enable seamless cross-border transactions, bypassing traditional banking channels. With many criminals operating vast international networks, it's increasingly hard to monitor and control the movement of funds across jurisdictions, allowing illicit activities to go undetected. Its inherent anonymity makes it increasingly hard for banks to perform effective customer due diligence and know your customer (KYC) processes with its current labor-intensive AML processes.

Poor data sharing has also proved to be a key failing, with banks operating on a siloed model lacking integration and collaboration. Criminals are taking advantage of this, creating complex networks of different names and addresses, for example, to remain untraceable from current AML detection tools. This inflicts greater pressure on AML compliance analysts, making it more challenging for financial institutions to scale their AML efforts.

AML compliance executives want platforms that can enhance risk identification and sharpen detection while maximizing investigator performance. To get here, investing in labor isn't the answer to tackling legacy transaction monitoring processes. Banks should instead be investing in technology to improve operations.

A new approach to trump fraud

Financial institutions are primed to defend themselves against illicit activity by adopting an AI-centric approach to maintain a critical edge over criminals at speed.

Our research revealed that over half (51%) of respondents believe that increased use of AI and machine learning is the future of AML and KYC programs.[8] With the potential to instantly analyze huge data sets across multiple networks, investigators can build a better view of the customer and work at speed to decipher if a transaction is legitimate. This is where AI is already helping AML professionals identify bad actors.

AI-powered AML offers the capability to produce a comprehensive customer risk score using machine learning. It excels in detecting nuanced connections between customer actions and possible AML warning signs, which might elude traditional, rigid rule-based systems. Furthermore, AI can enhance the efficiency of KYC verifications and customer due diligence processes.

The same is true for transaction monitoring and alert prioritization. By assessing and ranking the alerts generated by an AML monitoring system, transactions can be flagged as potentially suspicious. By adopting AI-based solutions, more effective patterns and anomaly identification will follow.

Machine learning can also help fill the gaps created by cryptocurrency's pseudo-anonymity. By extracting information from a blockchain ledger and reviewing the entire transaction history between public addresses, machine learning can uncover patterns that go unnoticed by humans, such as detecting how far removed a crypto wallet is from another account or finding wallets with ties to known high-risk sanctions links. By training a machine model to detect suspicious patterns, banks can get a clearer sense of which transactions are high risk and reduce the volume of false positives they encounter.

AI's unique prowess lies in its innate capacity for perpetual learning and adaptation through machine learning, enabling it to continually evolve in response to the ever-emerging strategies employed by financial criminals.

Investing in AI: Bridging the technology gap

Investment in the right technology is paramount. Financial institutions should prioritize investing further in AI-based solutions to help win the war against fraudsters and other bad actors.

Although the right investment will be crucial in tackling financial criminals, it will also free up the time of AML analysts to focus on identifying or uncovering real AML risks. It's a more cost-effective solution that helps counter the sky-high annual costs of operational compliance, allowing financial institutions to keep more money in their pockets and keep up with evolving or new typologies. Our research shows an appetite among AML professionals to embed AI solutions into AML processes; however, further investment is needed to bridge the current gap.

Financial institutions need to take a refreshed viewpoint on AML. They're sitting on a wealth of data they can use to better protect their customers and businesses. By possessing a more AI-centric strategy, they can put this data to good use, stopping criminals in their tracks before they can do any damage. This approach can potentially make compliance professionals' jobs far easier and more rewarding, but additional investment is needed before we see these fully embedded into AML processes.

Takeaways

- Criminals are evolving their methods, leveraging advanced technologies like generative artificial intelligence (AI) and cryptocurrencies to outsmart legacy anti-money laundering (AML) systems.
- Outdated transaction monitoring, high false-positive rates, difficulties tracking cryptocurrency transactions, and inadequate data sharing among financial institutions demonstrate why existing AML strategies are due for an upgrade.
- AI and machine learning offer a promising solution to enhance AML effectiveness. These technologies enable better analysis of vast data sets, more accurate risk assessment, improved transaction monitoring, and identification of suspicious patterns that evade current structures.
- Financial institutions must prioritize investing in AI-based solutions to bridge the technology gap. This investment not only aids in combating financial crimes but also allows AML analysts to focus on real risks while reducing operational compliance costs.
- Embracing an AI-centric strategy empowers financial institutions to leverage their data effectively, enabling proactive identification and prevention of criminal activities.

[1] Dow Jones, "What is the Thread of Financial Crime," Risk and Compliance Glossary, last accessed January 17, 2024, https://dowjones.com/professional/risk/glossary/financial-crime/threats.
[2] LexisNexis, "Global Spend on Financial Crime Compliance at Financial Institutions Reaches $213.9 Billion USD According to LexisNexis Risk Solutions Study," news release, June 9, 2021, https://risk.lexisnexis.com/global/en/about-us/press-room/press-release/20210609-tcoc-global-study .
[3] Feedzai, *The State of Global AML Compliance 2023*, August 2023, 5, https://feedzai.com/aptopees/2023/08/Feedzai-The-State-of-AML-Compliance-2023.pdf
[4] Deloitte, "Deloitte Banking Alert," February 2023, https://www2.deloitte.com/content/dam/Deloitte/ro/Documents/MC_Alerta%20AML-v2.pdf?nc=42.

[5] Lexology, “Anti-Money Laundering Trends and Challenges,” June 2020, https://www.lexology.com/library/detail.aspx?g=381280e4-7b9a-4a9c-beac-cda860430dee.
[6] Chananalysis Team, “Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022,” Chananalysis (blog), January 26, 2023, https://www.chainalysis.com/blog/crypto-money-laundering-2022/.
[7] Feedzai, *The State of Global AML Compliance 2023*, 5.
[8] Feedzai, *The State of Global AML Compliance 2023*, 5.