COSMOS
Navigate the Compliance Universe

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 Current monitoring alerts are outdated and can wrongly flag a Suspicious Activity Report (SAR).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.