The Journey to Complete and Connected Fraud & AML

Adopting a holistic approach to financial crime risk management

eBook

NICE ACTIMIZE

Xceed

NICE · ACTIMIZE

As many have fallen victim to fraud attacks and financial crime schemes in recent months, we're grimly reminded of the fact that criminals capitalize during times of crisis. With financial criminals becoming more sophisticated, financial services organizations must strengthen their defenses through discrete and connected analysis.

Read on to explore various technologies that provide powerful fraud and AML insights.

Access our recent ENGAGE All in One: AML & Fraud track sessions to hear about the latest trends and best practices to address your toughest challenges.

Watch Now ›

Table of Contents

Fraud and AML Boundaries Are Changing – For the Better

Many financial services organizations (FSOs) have historically drawn a distinction between anti-fraud and anti-money laundering (AML) efforts. However, boundaries are blurring, given the massive amount of data breaches and the explosion of cybercrime during COVID. Financial criminals continue sharing insights and collaborating on different schemes to create lucrative opportunities.

Where there is fraud, there's often money laundering. Therefore, FSOs need to adopt a holistic approach in connecting fraud and AML – driven by artificial intelligence – to give themselves a fighting chance against evolving fraud threats and sophisticated financial crime tactics.

Connecting fraud and AML can be interpreted differently at each FSO. For some, the investigation team may be managing both fraud and AML cases. For others, the two teams may be separated but collaborating on investigations. For example, the fraud team may send confirmed frauds to the AML team to create a case or file a Suspicious Activity Report (SAR). Regardless of where your FSO lands on the spectrum, the industry considers this connectivity an important element in the fight against financial crime.

Technologies, such as artificial intelligence and SaaS platforms, also play a crucial role in strengthening your financial crime risk strategy:

- Applying AI to perform discrete and connected analysis creates more actionable fraud and AML insights.
- Adopting a cloud-based platform enhances your speed and adaptability when responding to new threats.

NICE · ACTIMIZE

> *Fraud and AML technologies must be considered not in silos but as a continuum of enhanced lines of defense against modern financial crime.*

Watch Now >

Detecting Anomalies Through Discrete Analysis

NICE · ACTIMIZE

We're in an era where speed and customer experience are top priorities for consumers – and criminals know that. They are exploiting the fear of customer friction, while FSOs have accepted this as a cost of doing business. But effective fraud detection shouldn't be sacrificed for good customer experience. Applying machine learning to detect anomalies is a discrete way of distinguishing suspicious activities from normal activities.

- **Device Fingerprinting**

  Analyze device attributes, such as the operating system, configuration, IP address, and more, to build a digital profile for each user. Utilize AI-enabled analytics to discretely detect fraud prior to the point of transaction.

- **Behavioral Analytics**

  Monitor how the true user interacts with their device, along with usual transactions and activity. Unsupervised machine learning identifies anomalies from patterns of data – allowing FSOs to identify bot attacks, account takeover, and new threats they may not have experienced before.

- **Account-based Modeling**

  Instead of applying risk models to large customer segments, AI gives you the capacity to perform dynamic account modeling. This enables granular analysis, improving performance and fraud detection.

NICE · ACTIMIZE

> *Leveraging discrete, AI-enabled analytics empowers you to detect suspicious activities prior to a fraudulent transaction – without impacting the customer experience.*

Watch Now ›

Uncovering Linkages Through Connected Analysis

Criminals create various kinds of illicit entities to mask illegal activities, like creating shell companies to perform money laundering, terrorist financing, drug trafficking, or a myriad of other schemes. For example, the Panama Papers exposed that numerous shell companies were owned by politicians and some of the world's wealthiest people to commit fraud, evade taxes and avoid international sanctions. Looking beyond individual data points to find connections and linkages creates a clearer view into complex schemes.

- **Omnichannel Detection**

  Apply behavioral analysis across all digital banking channels and payment rails to detect sophisticated attacks. Omnichannel analysis eliminates blind spots and ensures multi-vectored attacks are detected.

- **Entity Linking**

  Assess and evaluate connections between data to uncover hidden relationships. Data visualization of large networks of relationships and complex data enriched with AI risk scoring can equip investigative staff with better insights and help them take appropriate actions.

NICE · ACTIMIZE

> *By combining data intelligence, AI and entity link analysis, financial institutions can augment traditional KYC processes by creating a multilayer of network relationships between customers, their organizations, supplier and business partners.*

Watch Now ›

Benefits of discrete and connected analysis

- Get the most holistic view of each customer interaction
- Enhance visibility and analytics across all channels and stages of the customer lifecycle
- Consistently stay ahead of the next fraud threat by leveraging AI and ML
- Improve decision-making across fraud and AML teams through collaborative investigations

Xceed: Comprehensive financial crime management powered by Always on AI

NICE · ACTIMIZE

AI related technologies are projected to save banks billions annually within the next half decade. Xceed, our always-on AI platform, is designed for financial institutions of all sizes, especially community and regional banks, to fast track their entry into the age of AI-driven banking.

Xceed helps FSOs strengthen their anti-fraud and anti-money laundering efforts with:

- Multi-layered, omnichannel analytics
- Self-learning models that adapt to real-time threats
- End-to-end customer monitoring and screening
- An all-in-one SaaS platform for investigations and regulatory filings

Begin your journey to complete and connected fraud & AML

Discover more insights on-demand

Watch Now >

See Xceed in action

Schedule a demo >

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

www.niceactimize.com