Why banks must use a holistic data-driven approach to fight a rising tide of financial crime and fraud

Today's financial institutions are in an unprecedented battle against a rising tide of financial crime and fraud and are struggling to keep up. The siloed systems and processes relied on to detect and prevent such crimes and enforce compliance are proving less effective as financial crimes become more complex and interrelated. They are inhibiting the very ability of financial institutions to detect, prevent, and investigate crimes and are now the target of exploitation.

As financial crime and fraud continue to evolve in complex ways, financial institutions must take a more holistic and data-driven approach that's in line with the changing threat landscape or face spiralling cybersecurity and compliance skyrocketing costs and a continued decline in the ability to operate.

The new normal

The operating environment for financial institutions has become more challenging over the last decade. As consumers and businesses have moved online at breakneck speed, the volume and complexity of digital transactions have skyrocketed. Ongoing digital transformations within financial institutions, accelerated by the Covid crisis in recent years, have also increased the potential attack surface for criminals to exploit. At the same time, criminals have upped their game, becoming more skilled and adaptive, seeking out the path of least resistance, and continually evolving their methods to evade detection.

Together, these overarching trends leave financial institutions facing somewhat of a perfect storm. A new reality where crime pathways are expanding and converging, and a growing number of sophisticated and well-funded criminals are persistently on the hunt for new targets.

Financial crime & fraud by the numbers:

$2 trillion

Illegally laundered around the world each year.

$213.9 billion

The total estimated cost of financial crime compliance across financial institutions worldwide in 2021 was $213.9 billion, up from $180.9 billion the previous year.

$3.78

Financial services firms now pay an average of $3.78 for every dollar lost to fraud, up from $3.35 in 2019.

£754m

Fraud cost UK bank customers alone £754m during the first half of 2021 – a 30% rise in the same period in 2020.

$10.6 billion

Fines for non-compliance with AML, KYC, data privacy and MiFID regulations against the financial sector totalled $10.6 billion in 2020, up 27% from 2019.

Mind the gap

Many financial institutions rely on disparate processes and siloed IT systems for detection, prevention, and compliance. These systems and processes differentiate between financial crime and fraud, dealing with crimes as separate and distinct problems under different systems, within various departments, often with no integration between them. According to a KPMG Global Banking Fraud Survey of 43 retail banks worldwide, 43% of respondents reported having no integration between fraud and financial crime compliance.

Typically, financial institutions view financial crime as a compliance problem managed by compliance divisions that handle Know Your Customer (KYC), AML and CFT programs. On the other hand, fraud is viewed primarily as a financial loss issue dealt with by detection and prevention systems programmed to recognise suspicious behaviours - where each type of fraud is processed separately under different departments.

While these systems and processes have served financial institutions in years past, the current complex and interrelated nature of financial crime and fraud is rapidly rendering them far less effective. To illustrate this point, let's use the example of a breach conducted by a sophisticated organised crime gang. Such a breach can result in the theft of customer financial data, leading to the laundering of funds through different banks and using these funds for illicit crime or terrorist activities.

In this example, fraud, money laundering, and terrorist financing crimes are all connected and interrelated. While the IT department may initially discover such a breach, they only have a limited view. Risk, Compliance, and other departments may also have critical information. In a siloed environment, there is no one to take charge of detection and investigations. Disparate processes and systems that don't communicate or share data make it difficult to see the bigger picture and connect the dots, inhibiting the prevention of such crimes.

The FCA has long advocated for Compliance and Risk Management Functions to take a data-centric holistic view of joining the dots arising from detections in individual systems and following the money trail end to end.

Adopting a holistic data-driven approach

Adopting a data-driven holistic approach is not about tearing down the current systems and processes. It's about bridging the gap between them and building a connection that enables financial institutions to share, leverage, and act on organisational-wide data insights in real-time. This approach allows institutions to identify tactics, techniques, and patterns of suspicious activities more efficiently and with far greater effectiveness. In return for enhanced detection and prevention capabilities, institutions can improve risk decision-making which ultimately helps support a better customer experience. They can also reduce monitoring and compliance-related costs.

Financial institutions need to up their game in establishing a data-driven holistic approach. Below are several key considerations:

- Take a big data approach. Establish a single data hub to consolidate, aggregate, and store enterprise-wide data.
- Incorporate link analysis and network graph visualisations to assess, view, and efficiently evaluate complex relationships between disparate data points and nodes.
- Use machine learning and artificial intelligence to evaluate large data sets in real-time using supervised and unsupervised models to detect and predict suspicious behaviours that would otherwise be difficult to unravel through human intelligence alone.
- Adopt business intelligence tools that combine business analytics, data mining, and data visualisations to provide contextual and compelling insights.

Eastnets provides a suite of solutions that enable financial institutions to bridge the gap between silos and leverage critical data insights to meet more complex, interrelated, and evolving threats.

Eastnets SafeWatch AML

SafeWatch AML is an AI-driven and relationship analytics solution that creates risk scores and identifies anomalous behaviours, providing financial institutions with a comprehensive tool for AML detection. This solution allows institutions to offer an extra layer of security to their customers by tracking current and historical transaction data, whether online or offline, to ensure that every suspicious transaction is detected.

SafeWatch AML turns multiple information streams into a single, clean intelligence source, with customisable business rules and scenarios to help institutions adapt even faster to new risks and regulations.

Eastnets Safewatch Screening

SafeWatch Screening is a SWIFT certified product for advanced sanction and watchlist screening that has been installed in over 360 banks worldwide and granted the SWIFT Alliance Plug-in label for its seamless integration with the SWIFT environment. The solution provides fuzzy matching watchlist screening for real-time transactions, customer information batch mode capabilities, and other ad-hoc screening requirements.

SafeWatch Screening solution allows for continuous monitoring of customer and financial messaging. It provides a central checkpoint for financial and non-financial traffic, whatever the format or transportation of the data, and enables compliance officers to view all alerts from all sources on a single interface. The solution includes several capabilities for reducing false positives such as matching scores, good guys, violation/ business rules, and a decision re-application feature based on algorithms for suppressing repetitive matches.

Eastnets PaymentGuard

Eastnets PaymentGuard is a robust, real-time, multi-channel fraud prevention solution that uses an advanced AI-powered detection model to handle complex and evolving fraud threats. PaymentGuard dynamically detects and prevents fraudulent payments by using machine learning to scan a historical database of customer data — including transactions, device information, and geolocations and intelligently model existing and emerging patterns.

Using PaymentGuard, financial institutions can improve fraud detection rates across all payment networks and channels and reduce false positives to save time and resources investigating false alarms. The PaymentGuard solution also enables institutions to keep up with novel fraud schemes as they continually evolve and comply with new regulations, including PSD2.

Eastnets PaymentSafe

Eastnets PaymentSafe offers a comprehensive suite of business, security, and technology updates to deal with every modern payment challenge. The solution enables financial institutions to simplify payment workflows by unifying and centralising all payment networks and messaging formats onto a single, easy-to-use platform.

PaymentSafe interacts with SWIFT, ACH and RTGS without any significant investment in infrastructure and is tailored to the needs of today's financial institutions. With PaymentSafe, institutions can quickly, securely, and cost-effectively centralise the Straight-Through Processing (STP) of multiple financial workflows and respond to new regulations and messaging formats with improved efficiency.

eastnets

About

Eastnets is a global provider of compliance and payment solutions for the financial services sector. Our experience and expertise help ensure trust at 750 financial institutions worldwide, including 11 of the top 50 banks.

For more than 35 years, we've worked to keep the world safe and secure from financial crime. We do it by helping our partners manage risk through Sanction Screening, Transactions Monitoring, analysis, and reporting, plus state-of-the-art consultancy and customer support.

Learn more at www.Eastnets.com