Are Financial Institutions Losing the Battle Against Fraud Prevention?

The explosive growth in digital transactions and real-time payments has intensified fraud risks and caused financial institutions to suffer skyrocketing costs and fraud-related losses. According to the Association of Certified Fraud Examiners (ACFE), financial institutions now lose approximately 5% of their annual revenues to fraud. In 2020, financial institutions paid an average of $3.78 for every dollar lost to fraud, up from $3.35 in 2019.

These figures are undoubtedly staggering, but they should come as no surprise. Most institutions continue to rely on human analysts and old rule-based systems that are inefficient and cannot effectively detect and prevent increasingly sophisticated and complex fraud patterns. With fraud risks set to evolve and intensify further in the years to come, financial institutions must innovate and continuously invest in intelligent technologies to ensure they stay one step ahead of fraudsters.

Digital, Instant, Open and Everywhere

The Coronavirus pandemic has accelerated a series of existing trends in payments. Ongoing shifts towards cross-border e-commerce, mobile, and real-time payments have hastened, causing a sudden and significant rise in the volume and complexity of digital transactions to unprecedented levels.

According to an eMarketer Global Ecommerce 2020 Report, there were 145.7 million more online shoppers in 2020 than in 2019. Today, there are an estimated 2.26 billion online shoppers globally, with the e-commerce market forecast to surpass $6 trillion by 2024. Mobile wallet adoption also rose sharply to a record high of 46% in 2020, with real-time payments jumping by 41% to 70.3 billion transactions globally.

Beyond the continued and accelerating shifts to e-commerce and digital payments, changing regulations such as PSD2 are forcing financial institutions to open their doors to third parties, exposing them to new potential fraud threats.

Top Fraud Risks

With more staff working remotely, and an acceleration in the volume and complexity of digital transactions, financial institutions have increased vulnerabilities, and fraudsters have more opportunities than ever before.

Insider Fraud

Insider fraud perpetrated by employees or IT vendors is tough to detect and can be highly damaging. According to a 2020 Cost of Insider Threats Global Report by The Ponemon Institute, the financial services industry is one of the fastest-growing industries for insider threats, with a 20.3% increase over two years.

Business Email Compromise (BEC)

Business Email Compromise, where an email gets sent to an employee, either from a hacked email account or a spoofed email address, is on the rise. A recent Covid-19 Benchmarking Report by ACFE found that 85% of respondents reported an increase in business email compromise in the wake of the Coronavirus pandemic.

Authorised Push Payment Fraud (APP)

APP fraud uses a combination of social engineering and phishing tactics to manipulate victims into authorising payments to accounts controlled by fraudsters. While increased adoption of real-time payments enables more consumers to experience the near-instant settlement of transactions, they have also made APP fraud more attractive to criminals who can instantly receive their payday. In the UK alone, APP fraud resulted in £479 million in fraud losses in 2020.

Account Takeover

Account takeover using social engineering tactics where a cybercriminal gains access to an account and uses the stolen credentials to complete unauthorised transactions continues to be a significant problem. Despite its unsophisticated nature, a report by Kaspersky Fraud Prevention found that every second fraudulent transaction in the finance industry was an account takeover in 2020.

Man-In-The-Middle

Man-in-the-middle cyberattacks where criminals intercept or alter online communications to steal information such as account details and credit card numbers continue to be a significant threat despite regulatory initiatives like PSD2 requirements for Strong Customer Authentication (SCA). Fraudsters continually evolve their methods and have more opportunities than ever as online or mobile banking services increase.

Using AI and Data Analytics to Fight Fraud

Fraud prevention within financial institutions has primarily involved integrating rules engines on banking information systems. Although this approach proved reasonably effective in years past, times have changed, and these systems are no longer fit for purpose. Consumer and business behaviours have shifted, and the global economy has digitised. Financial institutions require next-generation capabilities to successfully combat fraud today and stay ahead of tomorrow's evolving threats.

AI-based fraud systems enable financial institutions to carry out fraud prevention measures with more accuracy and in real-time. With increased speed and accuracy in fraud prevention, financial institutions can overcome the limitations of slower human analysts, who have a hard time identifying fraud, and tend to identify legitimate account creations and transactions as fraudulent. Moreover, AI-based fraud prevention systems can intelligently model existing and emerging patterns, unlike more inflexible rule-based systems trained on past behaviour patterns.

Data analytics using link analysis tools to evaluate complex relationships between millions of data points and nodes is an essential and intelligent way to assess big data. Link analysis provides deep contextual insights into relationships between customers, accounts, locations, and payment flows that cannot be identified through purely human-led processes.

Eastnets PaymentGuard

Eastnets PaymentGuard is a robust, real-time, multi-channel fraud prevention solution that uses an advanced AI-powered suite of detection models with embedded data analytics including an Investigator Tool to handle complex and evolving fraud scenarios. 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.

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