Point of View

How Financial Institutions Can Achieve a Robust Defense Against Electronic Payment Fraud

Financial institutions are fighting a growing threat of electronic payments fraud across a range of payment channels, from SWIFT, Fedwire, SEPA, and ACH to electronic funds transfers. Fraud techniques are many and varied, from malware and phishing, to batch file manipulation, account takeovers and internal fraud.

ACH fraud exposure in the United States is estimated to be more than $1.2 billion annually, based on a recent American Banking Association report. At the same time, wire transfer fraud is also a major concern for banks, with typical per-transaction losses in the U.S. estimated at more than $60,000 – 30 times that of a typical check fraud, according to the same American Bankers Association report.

Real-Time Electronic Payments Fraud Detection and Prevention Can Yield Benefits in Faster, More Convenient Payment Services for Customers

In addition to the growing exposure, electronic payment fraud is also becoming increasingly sophisticated, with cybercriminals frequently using multiple channels and payment methods concurrently to attack a customer’s accounts. As a result, the point solutions traditionally used to identify suspicious activity for specific payment types or access channels can no longer adequately protect institutions and their customers.

To effectively combat payment fraud across multiple mobile and electronic channels as well as meet regulatory requirements, banks need to invest in fraud detection and prevention systems that help enable automated, real-time monitoring of multiple payment types and channels, including online and mobile, and that are tightly integrated with their account processing platforms. Real-time analysis of transaction data is also needed to mitigate a wider range of fraud risks to help stop fraudulent transactions before financial losses are incurred.

Effectively Harnessing Transactional, Institutional and Customer Data to Prevent Payment Fraud

The ability to minimize fraud across multiple channels in the most efficient way requires effective collection, and analysis of a range of transactional, institutional and customer-level data. This data is enriched with known fraud data and trends, along with other institutional criteria, helping banks detect all types of anomalies, suspicious transactions and other fraud indicators. By taking this holistic, data-driven approach to fraud prevention, banks can focus all their resources on the two percent of transactions that are typically responsible for up to 100 percent of fraud risks. In addition, the 98 percent of transactions that are genuine can be settled quickly and securely, ensuring that customers receive an excellent experience.

The key capabilities required to mitigate payment fraud risks across all channels include:

Analytics and Predictive Modeling

Data analytics effectively integrate a range of transactional, institutional and customer-level data to understand each customer’s normal payment behaviors. This includes the frequency, velocity and size of the payments they usually make, as well as through which channels, such as online or mobile, they typically initiate electronic payments. If a particular transaction falls outside a customer’s normal behavior pattern, and exceeds institutional risk tolerances, alerts can be generated and forwarded to fraud analysts in real time for further investigation.
One of the most effective analytics techniques for preventing fraud is pattern recognition modeling. This uses pooled data on electronic payment transactions and fraud to help banks identify fraud patterns and identify transactions that have similar characteristics – flagging them as potential fraud. This technique, which can be further strengthened by using a consortium approach to pool data from multiple institutions, prevents fraudsters from using similar fraud techniques multiple times.

Data analytics also helps banks to differentiate between unusual customer transactions and fraudulent transactions, which represent only one in 80,000 ACH transactions. This ability to reduce ‘false positives’ (transactions that appear suspicious but are in fact legitimate) helps banks avoid the risk of declining good customer transactions and enables them to provide the best possible customer experience.

**Effective Use of Fraud Scenarios and Scorecards to Combat Emerging Fraud Schemes and Target Specific Fraud Types**

The best payment fraud systems consider a variety of fraud scenarios. These look at different risk indicators, such as unexpected international transactions or sudden changes in payment types or channels used by customers, and generate an overall risk score for each transaction.

This approach is critical for addressing ‘Flash Fraud’ threats. In these kinds of scenarios, criminals expose an unknown weakness in a bank’s fraud systems or processes and initiate as many fraudulent transactions as they can before the loophole is closed. The best fraud prevention systems help banks rapidly respond to vulnerabilities by defining and implementing business rules that can restrict the offending activity in real time.

As well as helping banks to enhance their fraud detection capabilities and identify emerging fraud schemes, customized risk scenarios and scoring enables institutions to fine-tune the logic for their “decline, hold or approve” strategy. Banks should also be able to deploy and update their risk strategies quickly and simply, without the need for specialist technical skills or external consultancy engagements.

**Multichannel Fraud Detection and Prevention**

Increasingly, hackers coordinate attacks using multiple interaction channels in an attempt to overcome traditional detection systems. In addition, denial of service (DOS) attacks and other attacks are often used to mask payment fraud on a network, requiring a more tightly integrated view of payments and broader network activity.

To achieve the multichannel coverage required, institutions need fraud-prevention solutions that have visibility into customer activity across all payment and interaction channels, including online and mobile, and that are closely integrated with their core payments platforms. This approach enables them to capture payments from all channels and apply the same, sophisticated fraud-prevention logic across the business.

**Real-Time Fraud Prevention**

To react to the speed of fraud, and help prevent financial losses, payment fraud systems must be capable of sub-second analysis of all the relevant risk scenarios and models. In addition, response messages should be sent back to the originating systems, with alerts created simultaneously for further review by fraud analysts.

**A Layered Approach to Fraud Prevention**

To minimize the risk of financial losses, and comply with regulatory requirements, institutions need to take a “layered approach” to fraud prevention. Fraud prevention “layers” should include:

- Sophisticated data analytics and risk scoring – Predictive models, scorecards and decision trees are used to identify fraudulent transactions and improve operational efficiency compared to conventional fraud-detection systems, thus improving both fraud detection rate and operational efficiency.

- Independent verification of electronic funds transfers – In the United States, the FBI is advising all banks and businesses to implement processes and technologies for validating wire transfers to help ensure they are not originated by fraudsters. Effective fraud systems should apply this rigorous due diligence across all electronic payment types and refer potential fraud to analysts for further investigation.
• Automated responses – These responses that enable suspicious transactions need to be suspended immediately, before losses are incurred.

• Alerting and workflows – Flag suspicious transactions to fraud investigators help manage alerts and cases effectively through their lifecycle.

• Trend analysis and reporting – This layer helps institutions to continually enhance their fraud strategies, focus on only the riskiest transactions and customers, and demonstrate ongoing compliance with regulatory requirements for fraud detection and risk management.

“By taking this holistic, data-driven approach to fraud prevention, banks can focus all their resources on the two percent of transactions that are responsible for up to 100 percent of fraud risks.”

The Need For Agility and Vigilance in a Changing Fraud Landscape

Every year, new payment channels emerge. In 2014, for example, Apple Pay was introduced, giving consumers a convenient way to pay retailers directly with their phones. While the solution provided extreme convenience, it opened banks up to increased fraud exposure. Within six months, some banks were reporting fraud rates of over 600 basis points, which is 60 times the level of traditional credit card fraud.

To identify and prevent evolving fraud threats, banks need fraud systems that accurately score transactions for fraud risk across a full range of electronic and mobile payment channels. This approach can help institutions better detect and prevent fraudulent transactions in the most cost effective way.

Based on sophisticated, real-time analysis of transaction and fraud pattern data, suspicious payments can be flagged immediately, however and wherever they are initiated. In addition, multichannel fraud prevention ensures that analysts can focus their efforts on the two percent of transactions that are typically responsible for 100 percent of fraud incidents – helping institutions maximize operational efficiency and lower fraud-prevention costs.

To optimize fraud prevention strategies, payment fraud systems should integrate seamlessly with a range of other fraud prevention systems, enhancing their capabilities. At the same time, automation of fraud detection and prevention processes is needed to help banks maximize operational efficiency and ensure that all cases of fraud are effectively managed and resolved.

As a final consideration, all financial institutions are affected by emerging fraud trends and techniques. By taking a consortium-based approach that shares fraud data between institutions, it is possible to optimize fraud prevention strategies over time and identify new fraud schemes and threats more quickly.

Client Profile

Payment Fraud Manager from Fiserv is the industry’s first real-time, cross-channel monitoring and detection solution for electronic payments. It is one of the most comprehensive solutions on the market today. It uses advanced inference techniques and pattern recognition models to identify and help prevent fraudulent transactions across all payment types and channels, including online and mobile.

To maximize fraud-prevention capabilities, Payment Fraud Manager can be integrated with Customer Risk Manager from Fiserv. integration offers valuable customer-level data, including customer demographics, balances and deposits, tenure at the bank, behavior scores, prior frauds, prior risky activity, online banking and mobile banking behaviors, increasing the accuracy of fraud detection and minimizing false positives.

Based on a combination of transaction-specific and customer-level monitoring, Payment Fraud Manager provides an advanced approach to fraud prevention, reduces administrative costs, and delivers new competitive advantage for banks.
About the Author
Mannie Da Silva has over twenty years’ experience in the payments industry with financial institutions and software companies in the U.K. and U.S. Mannie is a recognized industry leader in fraud and risk management enterprise solutions, analytics and operational consulting. Mannie is also a fraud consulting expert who has managed teams of fraud consultants and worked in client-facing fraud consulting roles.

Connect With Us
For more information about Payment Fraud Manager, call 800-872-7882 (North America), +44 (0)845-013-1000 (outside North America) or +65-6533-9288 (Asia Pacific), email getsolutions@fiserv.com or visit www.financialcrimerisk.fiserv.com.

Fiserv is driving innovation in Payments, Processing Services, Risk & Compliance, Customer & Channel Management and Insights & Optimization, and leading the transformation of financial services technology to help our clients change the way financial services are delivered. Visit www.fiserv.com for a look at what’s next now.