INTERNATIONAL INSTITUTE FOR ANALYTICS

Enterprise Research Service

## Discussion Summary

# Leveraging Analytics to Combat Digital Fraud in Financial Organizations

**December 2015**

**Interview Featuring:**

**David Stewart, Director, Security Intelligence Practice-Banking, SAS**

## Introduction

Digitization creates major opportunities for financial services – automating operations, expanding channels, delivering engaging customer experiences. There are corresponding challenges – unprecedented data and transaction volumes, channel control in electronic marketplaces, and preventing fraud when the fraudsters are technologically adept. To discuss the opportunities, challenges, and solutions around financial fraud in the digital age, IIA spoke with David Stewart, Director, Security Intelligence Practice-Banking at SAS Institute Inc.

## Q: How are financial institutions defining "digital" these days?

Digital business includes a variety of activities across financial services. If we think about consumer banking, the obvious things that come to mind are online banking services available to us via a web browser. In the last few years, most banks have also rolled out proprietary mobile apps targeted for smart phones and tablets. Those are two examples of digital access points that financial institutions control.

Then you have alternative payment service providers like PayPal and Venmo that interact with, or in some cases even ride on the rails of, financial institutions. With these intermediaries, the financial institution doesn't own the customer touch points or all of the security associated with a payment interaction. But the real digital disruption with respect to payments comes from Apple Pay, Samsung Pay, and the various telco and mobile providers that are creating their own payments infrastructures.

All that's on the consumer side. On the commercial side, financial institutions are talking to us about the digital aspects of how customers can move funds more rapidly through electronic funds transfer services like Swift, ACH, Fed Wire, and Chips. Both commercial and consumer banking are experiencing considerable growth in transaction volume, including tremendous growth in small-amount payments by consumers.

## Q: Please say more about the business challenges that arise with the expansion of digital business.

The first challenge for banks is to keep pace with innovation, and keep up with all the FinTech players that are creating alternative services, including payment platforms. A lot of these services are targeted at the millennial generation that has grown up with smart phones in their hands. The bank has to provide a frictionless interface, and create a positive brand experience, for young customers who may not understand basic concepts of banking.

With the proliferation of third-party intermediaries and FinTech services, another major challenge is risk and fraud. These players may not have the same security standards that the large institutions have implemented. They may not be PCI DSS compliant, for example, and that introduces a fair amount of risk. Financial institutions have to balance innovation with the ability to protect their customers because, at the end of the day, the big competitive advantage that traditional financial institutions have over the new payments providers is customer trust and protecting the customers against loss.

## Q: What are some specific risk and fraud scenarios that financial institutions need to avoid?

A good example is the risk incurred when a financial institution launches a product with new partners, even with a trusted and ubiquitous brand like Apple. Some of the early Apple Pay launch partners were institutions like Chase, Bank of America, American Express, Wells Fargo, Citi – all highly trusted brands in their own right. But there was a breakdown in terms of the know-your-customer authentication, when provisioning service via the smart phone. Early feedback had fraud rates as high as 6 percent, which is vastly higher than the three to five basis points of fraud losses in the credit card industry in the United States.

That just illustrates how you have to do your homework and look at all the potential risks that a financial institution may be exposed to when it does a product launch with a third-party. There are many, many players coming into the payments ecosystem, and a bank has to carefully

choose with whom to partner. Banks also have to reengineer the product launch process. Some have started innovation labs to attract partners. Providing new products and services to a new generation of customers on new digital platforms means taking risks. On one hand, banks have to do more product launches to see what works. On the other hand, they need the business product owners, fraud technology team, and fraud operations team at the table when launch decisions are made.

Another scenario to avoid is commercial account takeover. This past year we have seen a recurrence of attacks where cyber criminals compromise the credentials of an officer of a company, usually a small to medium-size business that may not have as much security technology or awareness as a large company would. The criminals compromise and steal the credentials with key loggers, man in the browser, or man in the middle attacks, and then in rapid succession wire money out of those commercial accounts, generally to high-risk jurisdictions off-shore, completing the theft intraday. The compromised systems are often automated payments networks that banks have set up for their commercial clients.

Commercial account takeovers are rare events, but the losses can be very high, and clawing back the funds from overseas can be very difficult. Because they're rare, it's also difficult to build predictive models on these events. Fraud modelers may choose to use a combination of unsupervised learning techniques to score abnormal transactions. Because of the velocity of these attacks, it's imperative to notice anomalous behavior as soon as it commences.

There are also account takeovers, of course, on the consumer side. Any time your credentials are compromised in an online session, someone may be able to steal part of your identity and apply for credit cards or unsecured loans. We just did a data quality study for a bank and found about 130 synthetic identities out of 4.5 million customers. So those things happen, but rarely. The fraudsters have really been going after the bigger fish in the commercial world, including breaching major retailers and financial services institutions where they can exfiltrate customer credentials and monetize them on the dark web.

The bottom line is that, in a more digital world, banks use more automated on-boarding and authentication processes and there's less human interaction and screening. And the speed of payments and services accelerates through digital channels. That introduces new layers of risk.

## Q: What are the challenges specific to growing data and transaction volumes?

The challenges are to scale up and speed up. Transaction volume is growing fast, especially in emerging markets. The number of mobile payments and person-to-person payments in markets like India and Kenya is skyrocketing. The amounts are very small, but if a fraud detection or prevention system needs to cover all transactions, the dollar amounts don't matter. The technology has to scale up.

Meanwhile, expectations are rising around the speed of payments settlement, whether it is the New Payments Platform in Australia, or faster payments in Europe, or proposed real time ACH in the United States. In Australia, the target latency for settlements in 2017 is six seconds. So we're going from settling payments intraday in a matter of hours to a window of six seconds or less.

Financial institutions need an orders-of-magnitude increase in what I call "decisioning scalability." Today we have clients using an on-demand scoring engine that can decision, at point of sale, peaks of let's say 3,000 transactions per second, which is very impressive. With newer event stream processing architectures, used now in the cyber world to detect advanced persistent threats on an entire network, we're testing at about 800,000 events per second. Banks are at a strategic inflection point, needing to modernize their systems to be prepared for the growth in data volumes and for real-time payments settlement.

## Q: How are big data and analytics being deployed to meet the challenges and reduce digital fraud?

The key to fraud detection in payments is making use of more contextual data. Not just data about the immediate transaction and online session, but about the device being used and how it's been used in the past, biometric identification data about the person using it, and data on that person's patterns of activity. So we need fraud detection technologies capable of

decisioning huge volumes of transactions in a much shorter period of time, using broader sets of data because we don't have that face-to-face interaction as in the brick-and-mortar days.

We're using a growing set of advanced analytical methods to work with that big data. We use different techniques for a problem like credit card fraud, where there are a lot of known frauds, versus commercial account takeover in an electronic funds channel. There we use more unsupervised learning or anomaly detection against a population because we do not have as many known frauds. We also look at methods like decision trees and random forests to compare how much lift our models get relative to more mature techniques like neural networks.

Machine learning has been the backbone of our advanced analytics strategy for the past decade. Lately, it has come into the common consciousness because of self-driving cars, but techniques like gradient-boosting have been in play in our fraud detection models for quite some time.

Very importantly, we're seeing a transformation in how we build models. We can deploy many, many more challenger models using a variety of analytic techniques, and build ensemble models that draw upon multiple techniques. In-memory architectures allow us to develop and test these models against much larger data sets, and run many more iterations of them during the development cycle. So model development gets faster and more agile and ultimately delivers higher quality results.

Finally, there's a transformation in how models are used, and it's all about visualization. Banks are looking not only at the performance of the models in production and how fast they can be built and refined, but also at how visualization can be used to see trends, simulate actions, and refine fraud detection strategies. They want to be able to visualize at a macro level to see where fraud activities are occurring, perhaps in a specific geography, and then make changes accordingly. Visual interfaces enable people to simulate changes in strategies, for example, for handling a rash of fraud events, and to perform what we call "visual rules estimation." Show me visually what the operational impact is going to be if I make a change in queuing or routing in my call centers. What impact is this going to have on my operational systems and my customers?

## Q: What are the more innovative financial institutions doing in fraud detection?

They're making better use of the contextual data I mentioned and creating more contextual awareness, both in cyber security and in fraud detection. If I'm in the middle of an online session after several failed authentication attempts, and I'm trying to initiate an international wire transfer, and I'm using a different device or maybe a device known to be associated with a fraud loss, and geo-location data that suggests I'm outside my regular footprint – all of these things provide context that should enable a system to generate a more accurate score.

The challenge, of course, is data integration, pulling in contextual data from advanced security systems, and syncing it up with data about the transaction and the customer in real-time.

The goal is a "digital decision hub" that can ingest different types of risk measures from different products, channels, lines of business, and access points including mobile, online, and traditional banking services. Then use that together with behavioral data, session data, device data, and increasingly biometric data, to score, at a point of sale, the likelihood that you are who you say you are, that this is a legitimate session, and that this is a legitimate payment attempt. And do all of that in about 50 milliseconds or less. That is where financial institutions want to go.

## Q: Who are the key stakeholders in financial fraud detection?

There are two major sets of stakeholders. First are the business executives who have P&L risk from fraud or who are trying to launch digital products and grow top-line revenue. Second are the people responsible for information security and fraud prevention. Ideally, there's an officer in charge of all security intelligence, including cyber security, fraud and money laundering, corporate security, physical security – all those unsavory risks to manage. More common is to have those responsibilities split. But regardless of the reporting structure, you need

representatives of information security, fraud risk management, and fraud operations at the table with the business owners.

The objectives of these stakeholders should be not only to reduce and prevent fraud losses, but also to improve customer service and grow revenue. For example, working with a large credit card issuer we were able to reduce their fraud loss by about $40 million annually. The models also significantly reduced their false positive rates, so there was much less referring or denying of good customers. An end-of-year comparison saw a revenue increase of about $60 million for that same card portfolio. The payback of good fraud detection can go far beyond loss reduction.

## Q: What else do the stakeholders need to know and do?

First, take a close look at what new technology architectures and big data analytics bring to the table. There's an imperative to scale up and speed up financial transactions and fraud detection. And there are opportunities to leverage big data analytics and even to reduce technology cost of ownership. But take a measured approach in how you adopt some of these technologies because we're dealing with mission-critical applications here, and downtime is not acceptable. You want to make fraud detection models and systems more robust and accurate without assuming too much risk associated with respect to new technologies, operational performance, and customer experience.

Second, develop a well-thought-out strategy for how to gather, integrate as needed, and utilize data that may cross several lines of business and technology organizations within an institution. The objective is to incorporate more of that contextual awareness into fraud detection. Given the variety of data potentially in play, you should take a measured approach here, too.

Third, leverage the power of visualization. If you can visualize problems at a higher level, you can more succinctly articulate where the risk exposures lie. You can also use visualization tools to communicate trends and potential exposures to stakeholders so they experience the benefit of big data analytics.

## Additional Information

To learn more about this topic, please **visit**.

## About the Interviewee

**David Stewart** is responsible for the development of strategy, guiding product management and supporting the marketing of SAS' fraud and financial crimes solutions for the banking industry. Stewart is responsible for coordinating best practices among SAS' global subject matter experts in combating financial crimes. He works closely with many of the world's most innovative financial services institutions, regulatory agencies, SAS research and development, implementation teams, and alliance partners to deliver superior solutions for fraud detection and complying with anti-money laundering regulations.

Previously, Stewart served as a SAS Business Manager at one of the world's largest financial institutions. He has worked exclusively with financial services companies over the last 20 years on various consumer risk, marketing and compliance initiatives.

Stewart is a Certified Anti-Money Laundering Specialist, serves on the North Carolina ACAMS board, and holds a bachelor's degree in economics from North Carolina State University.