Leveraging Analytics to Combat Digital Fraud in Financial Organizations

IAN HOLMES
Senior Manager, Security Intelligence Practice, SAS Institute

UPDATED APRIL 2019

Interviewed by Robert Morison, IIA Lead Faculty
How are financial institutions being digitized these days?

Digital business includes a variety of activities across financial services. In consumer banking, online banking via a browser-based web session is giving way to more agile interactions using a mobile or wearable device. Most banks have also rolled out proprietary mobile apps targeted for smartphones and tablets. We also see institutions rolling out digital-only offerings that may not directly reference their brand in order to appeal to a new market or audience. The innovators are beginning to harness voice recognition to engage customers through digital assistants or ambient engagement.

Digital disruption with respect to payments began with services offered by the likes of Apple Pay, Google Wallet. Then you have alternative payment service providers like PayPal, Venmo, and Alipay, and the various telco and mobile providers that are creating their own payments infrastructures. Zelle offers a variation, where the services have the option of being tightly coupled with institutions. With these intermediaries, the financial institution doesn’t own the customer touch points or control all of the security associated with a payment interaction.

On the commercial side, financial institutions are also modernizing their risk controls to support faster payment standards. Europe and Asia are further ahead; however, with Real-Time Payments (RTP) in the U.S., institutions are compelled to evolve. Both commercial and consumer banking are experiencing considerable growth in transaction volume, including tremendous growth in small-value payments by consumers as cash is marginalized.

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

The primary challenge for traditional banks is to provide better digital offerings and experiences to attract and retain a new demographic that has grown up with social media and a smart device. This is often difficult to achieve through the legacy technology in banks. Conversely, FinTechs are disrupting the status quo with apps that offer a frictionless customer experience and in many cases offer value add such as personalized financial advice.

The proliferation of third-party intermediaries and FinTech services opens another major avenue for exposure to risk and fraud. These players may not have the same mature security standards that the large institutions have implemented, and they are less concerned with reputational risk, instead focusing on market share and capital funding. 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 based on the fact that they will protect the customer’s assets.
What are some specific risk and fraud scenarios that financial institutions need to avoid?

Financial institutions need to improve their digital controls to combat fraud through Synthetic Identities, where fraudsters create composite digital identities gleaned from personally identifiable information available on the dark web or via social engineering. According to an industry survey, synthetic identity losses are expected to surpass $1.25 billion in 2020. As institutions move more of their account opening processes to digital channels, it’s becoming increasingly more difficult to verify the identity of the individual, especially if the applicant is new to the institution. It’s imperative to analyze device information, along with other consortium and system-of-record information to verify the identity and authenticate that through the account opening process. Leading institutions are also transforming their business processes to a risk-based authentication of the session and individual prior to authorizing payments.

Another significant risk is commercial account fraud. According to the FBI, between December 2016 and May 2018 there was a 136 percent increase in “Business Email Compromise” (BEC) fraud, totaling $12.5 billion during that period. In a BEC attack, 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 are still actively producing malware to 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. As the industry moves to faster payments, real-time prevention is required due to the shorter settlement periods.

Commercial account takeovers are rare events, but the losses can be very high, and clawing back the funds from overseas can be very difficult, often relying upon best efforts and inter-bank relationships. 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 and anomaly detection to score 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 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 digitized world, banks use more automated on-boarding and authentication processes with less human interaction and screening. And the speed of payments and services accelerates through digital channels. That introduces new layers of risk.

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

The challenges are to scale up and speed up. As commercial and consumer payments become easier and less costly through digital channels, and as these services are introduced to the traditionally “under banked,” transaction volumes are significantly increasing. We have made significant investments in Research and Development to meet the peak transaction demands of our clients in China, for example.
As faster or real-time payments are adopted globally, the settlement period has narrowed to as little as six seconds. Depending upon the jurisdiction, there may not be the typical claw back period to recoup fraudulent payments. Real-time decisioning that provides a high level of detection is absolutely necessary in a faster payments economy.

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.

**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 session, but also 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 orchestrating a variety of inputs on 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.

There is a lot of hype on the adoption of Artificial Intelligence in fraud prevention. Clients want analytics that adapt and learn from sophisticated attacks. We typically deploy ensemble techniques that use a combination of machine learning methods. Where we have a lot of known fraud events, such as card fraud, we deploy supervised learning. If we are monitoring for rare fraud events, such as commercial wire fraud, we also deploy unsupervised learning techniques to identify anomalous behavior on a payment, device, or beneficiary. The advancement in deep learning algorithms along with the advancement in compute resources means we can also run thousands of iterations with different algorithms, incorporate more features, and ultimately deploy better models to improve the digital customer experience.

Technology is changing so rapidly that traditional institutions are pursuing multiple strategies to keep pace. While SAS believes we provide superlative analytics, many of our clients want the option of being autonomous. If they are rolling out a new digital product, perhaps they want to deploy a model rapidly using SAS, R, Python, or Lua. We have opened up our platform with a “modeling harness” that allows clients or partners to deploy their own algorithms while preserving the governance and strategy management of the system. Many of our clients are also moving applications to the cloud, and we have refactored many of our algorithms for Cloud Analytics Services. Ultimately, we are giving our clients more options for how they deploy analytics at scale to keep pace with customer expectations in a digital marketplace.

**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 a digital 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 risk score.

The challenge, of course, is data orchestration, pulling in contextual data from bureaus, device reputation consortia, and biometric providers, 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. Our most innovative clients are scoring sessions, payments, and customers to make a
decision in tens of milliseconds so that honest customers are moved quickly through the green path. One of our clients is increasing revenues by $20 million annually through the use of customer scores within the decision stream. Declining fewer good customers drives Net Promoter Scores and ultimately profits.

What else do the stakeholders need to know and do?

First, recognize that AI is only as good as your data. The newest algorithm will disappoint if you don’t have a single view of customer behavior. We spend a great deal of time architecting our fraud decisioning platform with feature engineering at the forefront. It is imperative to understand how to incorporate multiple scores on multiple entities if we are going to deploy digital fraud models in tens of milliseconds.

Second, have a strategy for incorporating cross-channel information into your scoring and decisioning processes. If you have profile information on a customer’s behavior across other relationships, that baseline of activity can provide context within a digital session.

Third, use analytics and automation to continuously learn and improve your day-to-day operations. As we move to adaptive and dynamic machine learning strategies, firms can become more self-sufficient and agile at making adjustments to fraud strategies intraday. We have improved our simulation and estimation capabilities to empower clients to see the operational impact of changes in fraud detection strategies.

While customer expectations have grown with the move to digital commerce, the advances in computing power and analytics gives fraud stakeholders more weapons in their arsenal.

Additional Information

To learn more about this topic, please visit SAS Fraud Management.
About the Interviewee

IAN HOLMES

Ian Holmes is a Global Lead for Enterprise Fraud Solutions with the SAS Security Intelligence practice.

Previously, Ian gained extensive banking industry leading experience through fraud strategy roles, with specific expertise in payments fraud covering cards and application fraud. His career developed from the ‘ground up’ to embrace analytics and strategy. Ensuring the bank was best placed to prevent fraud attack Ian gained deep expertise of decisioning systems. Ultimately, Ian became Head of Card Fraud in the UK division of HSBC and was recognised globally by his contemporaries.

Joining SAS in 2011, Ian’s global role is to provide fraud expertise to drive the product enhancement; pre-sales and business implementation of the banking fraud solution globally. Ian’s team are SME’s and solution experts whom support current customers to maximise fraud performance as well as presenting business case capability to potential clients.

Ian’s fraud expertise is pivotal in retaining SAS’ recognition and reputation in the industry, supporting marketing initiatives and strategic collaboration with key third party vendors is key.