FRAUD ANALYTICS: PROTECT YOUR DATA, IMPROVE YOUR BOTTOM LINE
Not surprisingly, this need for speed is being acutely felt by all players in the payments ecosystem. The days when banks, processors, merchants and other intermediaries had days and even weeks to make a payments decision and settle a transaction are long gone. In today’s world of mobile, digital and immediate payments, transactions settle in minutes or seconds — putting enormous pressure on traditional fraud detection and fraud prevention solutions.

In the past, fraud attacks were relatively predictable and simple compared to today’s schemes. They moved at the pace of check settlement or the ability to generate a counterfeit, cloned credit card. Fraud analysts needed fewer data points to uncover what were mostly known forms of attack, and they could create and deploy rules to detect them relatively easily.

Today, however, business logic and institutional knowledge alone won’t cut it, and rules are just one of the necessary capabilities of a truly comprehensive fraud solution. In this new world, banks, processors and merchants no longer:

- **Know all the attacks.** Traditional rules-based fraud detection approaches are good at catching known fraud patterns, but often are ill-equipped to uncover new or emerging trends. Attackers change their tactics on a daily, hourly and even minute-by-minute basis. Payment system players need an efficient, effective way to sift through all the data, uncover emerging patterns and pinpoint new indicators of risk.

- **Have the luxury of time.** Fraudsters target the same collection of fast payment mechanisms as consumers, leveraging their speed and immediacy to alter attacks. This adaptability lets them fly under the radar of traditional rules-only fraud solutions.

- **Interpret all the data.** Usually, more data means more insight. While the move to digital payments, possibly with the complement of additional third-party data, means much more indicative information, it’s important to note that most fraud solutions cannot ingest more data without expensive and time-consuming third-party solution integrations. With so much data evolving and flowing through payment mechanisms, manual rule-entry methods cannot keep up, which means fast-evolving attacks are exploiting these gaps.
Enter analytics. To keep up with the speed of today’s payments ecosystem and the fast, ever-changing fraud attacks that go with it, banks, processors and merchants require a multi-faceted approach to fraud detection and fraud prevention — and that means integrating predictive analytics into the traditional rules-based mix for a blended and balanced capability.

As the name implies, predictive fraud analytics aim to help fraud analysts better predict in real time the likelihood that a given transaction is fraudulent. Using “big data”-types of technologies, predictive analytics automatically sift through huge quantities of financial and non-financial data to quickly and efficiently uncover anomalous patterns indicative of fraud — many of which may go undetected by rules-only-based systems and certainly human analysts alone.

**“LEARNING” BEHAVIORS — BEHAVIOR PROFILING**

For example, a bank, merchant or processor may use analytics to “learn” the typical behavior of a consumer, segment or group of consumers to better pinpoint anomalies. For the most part, humans are creatures of habit. They travel the same route each day to work from home, purchase coffee each morning at the same convenience store along that route, buy the same amount of gas at the same station at the end of the week and so on.

A good predictive analytics engine is able to take in all that data, correlate it across the individual or group and develop a baseline model of typical behavior. Then, when that individual or group’s behavior jumps outside the norm, it is recognized and alerted as anomalous — perhaps a customer initiates a series of wire instructions weekly, between 8 a.m. and 5 p.m., to a group of known beneficiaries, but then also attempts to initiate a wire to an unknown beneficiary for an amount that is 10x the average wire initiated over the last 90 days: that anomaly becomes an indicator of potential fraud. In that case, a well-tuned predictive analytics engine recognizes the anomaly and either denies the transaction in real time or flags it for further review, significantly reducing the chance of loss.

When combining behavior profiling with other fraud management tools, the institution increases its fraud detection and fraud prevention capabilities, while at the same time minimizing any potential impact on its legitimate customers.
markets or vertical segments, such as digital goods or online interactive gaming, that are notorious for fraud but difficult to segment out and account for with less adaptive solutions.

4 CUSTOM MODELS VS. CONSORTIUM-BASED MODELS

Predictive models for fraud detection can be developed based on the data of a single customer (issuer, retailer, processor) or they can leverage the data of multiple institutions and complement third-party data. In the first case, the fraud analytics solution can be tailored directly to the business using it, whether it is a small regional bank, a national retailer or a multinational card processor. A custom model is developed using only the data of the specific institution and its portfolio segments. The model, potentially using a combination of different algorithms to maximize detection, takes in a variety of inputs from multiple sources and synthesizes them to uncover complex fraud patterns and connections specific to that institution. Typically, a custom model is used only for the institution it was developed for and is not applicable to other customers.

An alternative to custom models is represented by consortium models, which are models developed on the data of multiple institutions. These models are typically used to provide fraud detection not only for the participating institutions, but also for institutions that were not part of the initial consortium. In both cases, the fraud detection performance obtained using the consortium model is related to the similarity between the fraud and genuine patterns present in the data of the individual institution using the model and the patterns present in the data of the consortium institutions. The more similar the patterns are, the more effective the consortium model is likely to be as a fraud detection tool for the specific institution using it. Consortium models can be shared among institutions with a shared geographic, industry or product focus.

The decision to use a custom or a consortium model can be driven by several factors: not only technical issues tied to the data characteristics, but also business considerations such as cost and time to deployment. An existing consortium model can be deployed immediately at a new institution, while a custom model will require some additional development time. While custom models are typically preferable for maximizing fraud detection, the individual circumstances and needs of a specific institution might dictate a consortium solution. In some cases, a consortium model can also be used as a temporary measure while an institution-specific custom model is being developed. In other cases, a consortium and a custom model can also be used together in a complementary fashion.

5 RULES HAVE THEIR PLACE

Still, predictive analytics cannot do the job alone. While analytics can be leveraged to do the heavy lifting required to sift through the mountains of data and uncover sophisticated fraud patterns, they are not the most efficient tool to protect against many common fraud vectors. For example, rules are critical at preventing fraud from known incidents, such as when hackers breach large retailers (e.g., Home Depot or Target) and steal troves of consumer credit card numbers. Fraud analysts can simply write a rule to deny any transactions using those stolen numbers, effectively blacklisting them and stopping fraud in its tracks, no analytics required. Often, fraud analysts will rely on a custom rules-based approach to immediately respond to a flash fraud incident that has been uncovered. As a result, the best solutions invoke a multifaceted approach which integrates both a predictive analytics capability with the more traditional rules-based engine.

6 GETTING THERE: MAKING THE ANALYTICS BUSINESS CASE

While using predictive analytics in concert with rules-based strategies is the best way to ensure all fraud — whether it’s known or unknown, fast moving or slowly evolving — is detected and prevented before losses accrue, some organizations are reluctant to move to a sophisticated analytics-based fraud detection and prevention system. Those that have gotten by until now using rules-based systems alone may have
trouble justifying the extra cost — in time, effort and investment — that implementing such a sophisticated solution may entail. Others may question whether they have the expertise on staff to manage a full-featured fraud analytics platform.

ROI IN MONTHS
First, let’s address the cost question. The whole point of a fraud detection and prevention system is to reduce losses from fraud, especially when losses are increasing rapidly due to newer, faster methods of payment and the newer, faster methods of fraud that frequently follow. Businesses that are hemorrhaging money in this new environment need to stop the bleeding — and fast. In general, payment players accustomed to rules-only systems can recoup their initial investment in a full-featured predictive fraud analytics solution in a matter of months. In fact, as they quickly fine-tune their detection capabilities, lower their false positive rates and reduce their fraud losses, many realize their savings sooner.

MORE TRANSACTIONS, MORE BUSINESS, MORE PROFITS
Furthermore, the business case isn’t all about loss prevention. Banks, processors and merchants that implement the right fraud analytics solution can also reap significant improvements in customer service, and ultimately, their bottom line.

This is because applying analytics to fraud detection enables consumers to have a better experience. Since the addition of analytics helps improve fraud detection while lowering the false positive rate, the banks and merchants gain greater customer loyalty as consumers are able to transact in confidence with less interruption. No consumer likes to deal with the fallout of their account falling victim to fraud. In the card industry, while the bank or processor will undoubtedly stop the fraud, cancel the card and send out a new one “in three business days,” the resulting inconvenience often erodes customer loyalty. According to “The ACI Worldwide Global Consumer Fraud Survey” prepared by Aite Group, approximately 20% of consumers that experience fraud severed their relationship with their bank or merchant. Furthermore, 40% of consumers whose cards were used to perpetrate fraud end up using their replacement card less, resulting in a significant drag on the business. Consumers are increasingly relying on their banks and merchants more to protect them as they experience more fraud. The study indicated an increase of consumers experiencing multiple fraud events in the survey period. In summary, based on the trends, catching fraud and improving false positive rates means fraud analytics helps avoid these scenarios of decreased customer loyalty.

In addition to avoiding the replacement card scenario, customers will also see that more of their transactions are being accepted quickly and that the bank, processor or merchant using the fraud analytics system is able to process more transactions regardless of the channel — in-store, online, mobile, etc. — they choose. In effect, analytics makes fraud detection more accurate, making it easier for businesses to serve
their customers more efficiently and in turn, do more business. At the end of the day, these businesses are able to both retain current customers and secure new ones. In the fast growing eCommerce world of online and mobile, conversion rates are improved, yielding significant new sales to complement the client satisfaction.

NEW OPPORTUNITIES
In many cases, analytics can also help businesses explore new opportunities and establish new business lines. More accurate fraud detection serves to provide a level of confidence required to enter new customer segments, geographic markets and even new product categories that in the past may have represented too much risk to consider. For example, many entertainment companies that previously shied away from new businesses, like online gaming, may reconsider a market entry or expansion once they are able to better manage their risks.

CARE AND FEEDING
Even with reduced losses, a superior customer experience and new opportunities, many businesses may feel unprepared to manage and maintain a full-featured predictive analytics-based fraud detection and prevention solution. Their staff may have no expertise in building data models, tweaking algorithms, monitoring machine-learning techniques, etc., and they may not have the necessary funding to hire and manage high-level data scientists.

The good news is they don’t have to. Market-leading analytics solutions should be flexible enough to meet the needs and expertise of any business. Those with the requisite skills and capabilities are able to purchase and field a full-featured solution that they can implement and customize to meet their needs, while alternately, businesses with fewer resources should be able to have a full-featured solution hosted and managed for them. A hosted option ensures that not only do all customers receive the breadth and depth of features they require, but their transactions are monitored by a provider that is both expert in predictive analytics/fraud detection and the entire payments ecosystem. A hybrid approach is also available, with the hosted or SaaS-based solution relieving the implementation and maintenance burden while providing the analytics and rules-based capabilities for a client’s risk management team to tailor and implement their risk strategies.

RETAILER REDUCED FRAUD

REDUCED ITS CHARGE-BACK RATE TO JUST 0.05%

REDUCED ITS DENY RATE TO JUST 3%

while seeing no increase in fraud levels

INCREASED MOBILE SALES without experiencing increased fraud losses

WHILE INCREASING SALES ACROSS MULTIPLE CHANNELS
DATA ANALYTICS PRODUCES ROI
Fraud attacks are no longer simple and predictable. With faster payments, advanced technology is essential to stay ahead of the attacks. Engaging a multifaceted approach to include predictive analytics, behavior profiling, consortium-based models and machine learning in combination with your existing rules-based system will not only block new fraud schemes, but it will reduce the trend of losses that you are presently experiencing. If that wasn’t enough to motivate an upgrade to your fraud management system, the ROI to be realized surely seals the deal. It is proven that today’s combined approach of data analytics and actionable intelligence uncovers new business opportunities with your existing customer base. Add the improved customer experience that is gained and you have a home run for a business case!

ACI has the depth and breadth of expertise required to maintain a leading-edge predictive analytics fraud detection and prevention solution that addresses the payments industry’s market challenges, both now and for the future. With more than 20 years of experience in the fraud analytics space (and the patents to prove it), ACI is continuously in the process of improving and investing in its solutions, including constant research in new technologies and capabilities, and is consistently ranked a leader by analysts in the fraud analytics space.

Its primary differentiator, however, is its proven domain expertise in payments, with the requisite breadth and depth to serve the entire payments ecosystem, from retail banks and commercial banks, to processors and other intermediaries, to merchants.

Many competitive fraud analytics offerings focus on one niche or another, but ACI is one of the few companies to encompass the whole ecosystem end to end and has access to data from every type of business serving the payments industry. It can readily apply its expertise across that full data set, enabling customers to analyze financial and non-financial events from multiple perspectives, significantly mitigating the risk of fraud — no matter how fast, unique or stealthy the trend appears. Learn more: ACI Proactive Risk Manager™ and ACI ReD Shield™

ACI Worldwide, the Universal Payments (UP) company, powers electronic payments for more than 5,100 organizations around the world. More than 1,000 of the largest financial institutions and intermediaries, as well as thousands of global merchants, rely on ACI to execute $14 trillion each day in payments and securities. In addition, myriad organizations utilize our electronic bill presentment and payment services. Through our comprehensive suite of software and SaaS-based solutions, we deliver real-time, any-to-any payment capabilities and enable the industry’s most complete omni-channel payments experience.