BUSINESS-DRIVEN FRAUD MANAGEMENT: ENGAGING WITH LEADERSHIP TO DRIVE INVESTMENT

February 2017
## TABLE OF CONTENTS

Executive Summary .................................................................................................................. 4
Overview ................................................................................................................................... 4
Key Findings ............................................................................................................................... 5
Financial Services ...................................................................................................................... 7
   Key Performance Indicators: Financial Institutions ................................................................. 7
   Key Performance Indicators: Card Issuers ............................................................................... 8
Factors That Drive Change in KPIs .......................................................................................... 10
   Digital FI ................................................................................................................................. 10
   Regional FI .............................................................................................................................. 11
   Card Issuer ............................................................................................................................. 11
Communicating With Leadership ............................................................................................... 11
Working With Information Security .......................................................................................... 13
Influencing Investment Decisions .............................................................................................. 13
Retailers .................................................................................................................................... 15
   Key Performance Indicators ................................................................................................... 15
   Factors That Drive Change in KPIs ......................................................................................... 16
   Communicating With Leadership .......................................................................................... 17
      Mature: Multichannel Retailer .............................................................................................. 17
      Developing: Marketplace Retailer ....................................................................................... 17
   Working With Information Security ....................................................................................... 18
   Influencing Investment Decisions .......................................................................................... 19
Conclusion ................................................................................................................................. 20
Recommendations ..................................................................................................................... 20
FOREWORD

This whitepaper, sponsored by RSA explores the challenges faced by fraud practitioners in effectively communicating fraud threats and trends to senior leadership, along with best practices in the financial services and retail industries for securing buy-in on new initiatives and technology investments. The whitepaper was independently produced by Javelin Strategy & Research. Javelin maintains complete independence in its data collection, findings, and analysis.
EXECUTIVE SUMMARY

Overview

In the financial and retail industries, effectively managing enterprise fraud risk is ultimately a three-step process: measure, communicate, and act. For a non-practitioner, this process can appear simple; however, in practice, getting each step right can be a long, complex exercise of trial and error. In this report, Javelin explores how different types of organizations in these industries go about each of the three steps, diving into their respective challenges and motivations and uncovering best practices and pitfalls. Optimizing the fraud management process isn’t easy, but it can mean the difference between securing buy-in from senior leadership and being underequipped to repel new and significant fraud threats that threaten the profitability and reputation of the business.

The Three Stages of Business-Driven Fraud Management

- **MEASURE**
  - Determine the right metrics
  - Create standardized reports
  - Benchmark against peers

- **COMMUNICATE**
  - Liaise with Information Security
  - Shared reporting
  - Regular meetings
  - Team member exchanges
  - Report to Senior Leadership
  - Monthly reports
  - Regular meetings
  - Emergency sessions

- **ACT**
  - Determine the necessary remediation steps
  - Institute new processes, if needed
  - Purchase new technology, if needed
  - Implement remediation plan

Source: Javelin Strategy & Research, 2017
KEY FINDINGS

The three KPIs that consistently matter to senior leadership are fraud losses, expenses, and the impact on the customer. These metrics represent the baseline for managing fraud by measuring the bottom-line impact. Communicating the numbers and tying them to financial performance allow senior leadership to understand the changes and enable the business units to understand the return on investment and act on new fraud solutions. Customer impact or experience is just as critical as the losses. Negative customer experiences will result in reduced revenue and loss of that customer’s acquisition cost.

Loss and expense metrics are important for motivating change, but don’t underestimate the influence of intangibles such as reputational risk. There are few things worse than opening the morning paper and learning that your organization had a breach or has been part of a significant fraud event. Even if the situations are “relatively” small and manageable from a risk standpoint, the public is highly aware of fraud and cybercrime. These events affect your customers and the people they talk to. On a broader scale, they affect the organization’s reputation in the market and consumers’ decision to do business with the organization.

When setting targets, organizations look beyond their own historical performance to the broader industry and compare peer performance. It is easy for organizations to get caught up in their own perceptions of performance. Engaging peer networks, seeking out research, and talking to vendors about industry performance can highlight areas for improvement, along with early indicators of up-and-coming risks. Industry benchmarks are the minimum performance levels, and management’s goal should be set to outperform them and consistently make improvements.
Network-level attacks bring info security and fraud teams together. Digital channels have become ground zero in the fight against fraud. Data breaches and faceless, automated attacks are a relentless burden on organizations of all shapes and sizes. This has required a much closer working relationship between information security and fraud management. What looks like benign activity to one group may be a significant problem when viewed holistically. Ultimately, making the smartest decisions on new investments for mitigating these risks requires both teams to be at the table.
FINANCIAL SERVICES

Key Performance Indicators: Financial Institutions

Confronted with an environment in which government regulations and low interest rates have placed serious pressure on banks’ earnings, FI fraud teams are expected now more than ever to stem losses while controlling costs. So, it is unsurprising that when it comes to measuring KPIs, the metrics that are communicated most to senior leadership are net fraud loss, loss avoidance, customer impact, and operational expenses.

FIs measure their net fraud loss and loss avoidance (prevented and recovered) across channels, including ATM, online, mobile RDC, call center, and branch, and by product such as ACH, check, debit card, and wire. The net fraud loss KPI can be further delineated into the specific types of fraud occurring in each channel, such as account takeover (ATO), and with each product, including counterfeit card, lost/stolen card, card not present (CNP), check forgery, counterfeiting, alteration, and kiting.

Among the most expensive and insidious forms of fraud, ATO is on the rise with losses jumping 61% from 2015 to 2016.1 As a result, measuring the overall rate of completed ATO is not enough for some FIs. One digital FI in particular also measures ATO by uncompleted attempts and profile takeovers. A profile takeover is when the account is accessed but money movement is not attempted. Detecting these events can help FIs stop fraud before losses can occur. On the flip side, measuring and examining ATO attempts that were not completed provide insights on areas where the FI is having some success — helping to justify previous investments and process changes.

Operational expenses are typically reported in a similar manner as fraud losses, but measuring the impact of fraud on the customer experience may require a more nuanced approach. The risk profile for each product, channel, or even

---

customer segment can differ significantly, requiring fraud management costs to be measured individually. And while the impact on customer experience could include measuring false-positive rates for POS and CNP transactions and holds on deposits, FIs may also monitor verification of documentation during onboarding, inbound call abandonment rates, and remediation time on cases.

Understanding how their industry peers are performing can be extremely useful for fraud teams seeking additional investment or touting the effectiveness of their efforts. But while some FIs leverage industry benchmarks to determine where they stand relative to their peers, there is a lack of reliable information on certain types of fraud. This is due to the diverse nature of FIs where different approaches to managing lines of business can affect the way that fraud is tracked. For example, one FI may place a counterfeit check ATM deposit in the ATM fraud bucket, while another one would place it in the check fraud bucket — with other FIs placing it somewhere in between.

**Key Performance Indicators: Card Issuers**

Existing-card fraud is a major component of consumer financial fraud and, its incidence rate has jumped over the last twelve months. As the stewards of consumers’ existing-card accounts, payment card issuers are on the frontlines of fraud protection in a highly active zone. Yet preventing and detecting fraud are not the only priorities card issuers face. There is also a delicate balance to strike between minimizing fraud losses and avoiding adverse effects on the customer experience. As such, card issuers’ KPIs consist not only of fraud losses and operational expenses related to fraud prevention, but also the impact of customer controls and decline rates on the customer experience.

Card issuers lean heavily on historical customer data to identify fraud risk indicators and build algorithms to flag transactions. To ensure accurate models, issuers measure fraud events and losses extremely closely, tracking changes in

---

fraud losses in basis points. While these models adapt over time and adjust to long-term fraud trends, issuers are occasionally faced with sudden and potentially devastating “flash fraud” events in which criminals uncover and capitalize on a specific vulnerability. In these instances, issuers are able to introduce new rules to their algorithms to immediately begin flagging attacks of that specific nature.

Developing and managing these systems take sizable investment and support staff. Operational costs can be steep for maintaining these systems, but some issuers are working to minimize operational costs in other areas. For example, they are eliminating fraud analysts who contact customers directly when fraud is suspected. In their place, they are automating customer contact through SMS alerts or push notification alerts. Thus, issuers not only minimize costs, but they also receive higher response rates (and quicker responses). They also benefit by more accurately identifying fraud and avoiding false positives.

Issuers differ from FIs in that they do not have the advantage of stickiness in the services they provide customers. While FIs build deep relationships with customers through cross-selling, and benefit from those relationships through multiple revenue sources, issuers’ relationships with customers are often transitory. Most consumers carry multiple cards, and while they may prefer one over the others, this preference is highly shakable and a card’s top-of-wallet status can be threatened by a single fraud event or inconvenient decline.

The vulnerability of consumers’ card usage to fraud and false positives has several consequences. When a consumer stops using a card altogether, the issuer loses all future interest and interchange fees on that card. This long-term proposition underlines the imperative to reduce friction in the customer experience, even at some cost. To better gauge their top-of-wallet vulnerability, issuers may track the customer impact of transaction declines using the net promoter score. Additionally, issuers will often consider the amount of interchange on a suspicious purchase when weighing the decision to decline or not, balancing what they risk to lose from fraud against the expected loss from the purchase or customer relationship.

“Nobody does OpEx the same way, so it is hard to benchmark that across the industry, but the bank wants to know if you are getting more or less expensive over time.”
- Fraud Exec, International Card Issuer

“We do surveys of customers that we specifically impact at the point of sale with a decline. The scores are significantly lower than a customer service call, but that is who we speak with.”
- Fraud Exec, International Card Issuer
While businesses and payments going digital comes with risks, it also provides ample opportunity for the parties involved in a payment to share information for increased accuracy in fraud detection. In addition to card usage data and fraudulent purchase attempts, issuers leverage the digital channel to identify suspicious activity, including account takeovers. Much like FIs, payment card issuers often monitor their customers’ online and mobile account access in order to track failed login attempts and interdiction rates. It is also increasingly important as consumers move card credentials into third-party wallets (e.g., Apple Pay), which issuers monitor pass/fail rates for enrollment, along with fraud volume related to mobile wallet transactions.

Factors That Drive Change in KPIs

The financial sector has pioneered the adoption of big data as a strategic tool for security and operations. However, once systems for collection and measurement are established they can become resistant to change, and the importance of flexibility cannot be understated in a changing fraud environment. Players in the financial market shared some of their experiences developing new metrics when new trends emerged or existing metrics became stale:

Digital FI:

- An executive saw an opportunity to better understand customers’ experience with fraud controls and identify pain points, an issue that touched on both operational risk and customer experience.
- Both departments came on board during a joint meeting, where the executive suggested collecting the following data:
  - The number of holds on transactions that result in returns or abandoned purchases
  - The overall card decline rate
  - Pass/fail rates on online account logins
  - Service level in the call center
- As a result of these metrics, a new KPI was developed that allows the FI a more intimate understanding of how fraud and declines affect business.
Regional FI:
- Quarterly meetings are held to review the performance of existing fraud metrics.
- Any meeting attendee can suggest changes to the metrics.
- Ownership of new metrics lies with a single person who defines, creates, and implements the metrics, as well as measuring their performance.
- It is important to have this formal space for suggesting new metrics, but a more flexible system would have a continually open avenue to revise and update metrics.

Card Issuer:
- Card issuers face some of the most slippery and rapidly changing fraud attacks, and small changes in trends that elude existing metrics can quickly add up to millions of dollars in losses.
- In the fraud environment for issuers, it is important that measurements are frequent as they are accurate.
- One card issuer moved from monthly to daily reporting across the account life cycle, statistically comparing daily reports to rolling 30-, 60-, and 90-day metrics.
- This issuer also records suspicious login data to get an early read on when there is an attack or process issue.

Communicating With Leadership

As fraud reporting has risen to the boardrooms of FIs and card issuers, there is more formality in the reporting process and awareness of the impact to business. FIs and card issuers both report on a monthly and quarterly basis.

Regular reporting serves a dual purpose in maintaining a close relationship between fraud teams and the boardroom. First and foremost, it ensures that leadership is appropriately informed of significant new developments, whether these are the continuation of previously observed trends or new schemes that are stressing existing controls. Second, it ensures that leadership is kept informed when business is progressing normally, expanding communication with leadership beyond funding requests or times when antifraud measures are under notable stress.

“If I can manage it in my own shop then it is just a communication (to senior leadership), but if I need money then that is a different story. We don’t make the presentations pretty – we get the right people in the room, fund it quick, and get it done.”
- Senior Fraud Exec, Digital FI
• **Start at the top**: One digital FI sends the monthly report on fraud losses and current trends to the operational risk committee, which includes the head of fraud, head of compliance, general counsel, and president. The quarterly report is sent to the board, and the head of fraud addresses the board when events are significant. There is also a board risk committee, which the head of fraud will engage when something happens outside the FI’s risk tolerance.

• **Start with the experts, and then communicate upward**: Another regional FI has monthly meetings between the enterprise fraud council and the operational risk council, with the outcomes sent to senior leadership. The fraud management leader also meets quarterly with business line leaders to present the scorecards for their products.

While regular updates for senior leadership are indispensable, when a significant fraud event has been detected or is unfolding, there is a need for immediate communication with the senior leadership. Like with periodic fraud reporting, it is important to have formal processes for determining which fraud events are escalated to leadership and the channels to use for escalation.

• **24 hour or less reporting**: One card issuer has a formal policy to report a fraud event within 24 hours when it meets certain criteria. This can be challenging because the totality of the situation may not be clear in that time frame. The message is communicated through the fraud management organization to the executives. The situation is assessed based on customer impact, PR impact, as well as fraud losses.

• **Internal fraud hotline**: Another FI uses an internal hotline for employees to report recently identified or rapidly unfolding fraud issues. The information is immediately routed to the business line leader to weigh the risk and exposure. While less useful for communication with senior leadership, these kinds of internal hotlines can be used to gather information from employees in areas such as the call center that see new fraud schemes firsthand and may be able to provide early indications of new schemes or tactics.
Working With Information Security

As FIs and issuers go digital, so do the criminals. With more and more fraud coming through data compromises and network-level attacks, fraud teams leverage their information security colleagues to more quickly react to threats and better protect their customers.

As with interacting with senior leadership, integrating data from information security teams through regular communication is essential. One issuer’s information security team publish a daily update of cyber events from the prior day. Statistics are provided on the number and types of incidents, along with highlights by region and any cyber news that hit the wires. The information security team also provides monthly briefings and an annual report.

A digital FI’s information security team and fraud team have monthly metric reviews from both sides of the house. Network-level attacks are shared as part of the cyber threat operations update. Day-to-day communications are strengthened with team members participating on each other’s teams to understand how network-level attacks affect customers and result in fraud. When the information security team has an inquiry on a fraud event, it knows exactly whom to contact on the fraud team for assistance.

Influencing Investment Decisions

Typically viewed as a cost center instead of a profit center, the fraud team faces significant challenges securing funding from senior leadership for new solutions and initiatives. Success requires a Lingua Franca, or common language, which can be used to deliver the most persuasive message. For FIs and issuers, this starts with the four common KPIs, which then are tailored and supplemented to meet the unique needs of their organization.

- **Develop a formal reporting process.** Institutionalizing the process of escalating fraud reporting and funding requests to upper management can ensure that buy-in across core stakeholders is accomplished. One fraud team
at a digital FI described its process. First, it worked with the CFO to examine the process of collecting and reporting fraud loss information. The CFO’s involvement and buy-in are critical. Then the team looked at the net fraud losses and anticipated what not implementing a solution could cost. The team used this effectively when analyzing its EMV rollout investment.

- **Reduce metrics to their simplest component.** Developing even a rudimentary return on investment (ROI) calculator can help in reducing an array of stats to a single figure that can be used in pitching new fraud investment. A major card issuer uses this type of tool to determine fraud investment feasibility. The calculator looks at the value of fraud application avoidance, zero-balance closures, revenue on declines, and more to reach a net save calculation, which is then divided by the operational costs.

- **Build in flexibility where possible.** One regional FI maintains separate funds for investments to address potential fraud events. While this approach spares the fraud team from having to escalate every challenging fraud scheme, it also requires supervision to ensure that these funds are appropriately applied to new schemes that cannot be addressed with existing resources.

For card issuers and FIs alike, fraud teams need to fight for resources, especially as the fraud management teams and investments are viewed as costs. Creating KPIs that senior management understand makes it easier for everyone to have a positive impact on the bottom line.
RETAILERS

Key Performance Indicators

Retailers are under tremendous strain from rising CNP fraud. Card networks place the liability for CNP fraud on merchants, motivating them to invest heavily in fraud prevention technology and operational teams. Retailers also face cyber threats to their networks as criminals attempt to compromise customers' account credentials and payment data. Not surprisingly, retailers measure, communicate, and act on almost the same KPIs as FIs and card issuers. All things considered, retailers and issuers are different sides of the same coin.

For retailers, fraud loss is typically measured as a percentage of sales across all of the channels where they conduct business, including the physical store, website, telephone, and the hybrid “buy online, pick up in store.” The fraud loss performance is compared with the budgeted plan for each channel. Marketplace retailers, including Amazon, Bonanza, eBay, Etsy, Newegg, and Rakuten, rely on sales commissions for promoting products, which makes not only dollars lost to fraud but also lost sales commissions useful metrics for assessing the impact of fraud on their businesses.

Retailers rely heavily on customer experience, knowing that there is a fine line between a repeat customer and an abandoned cart. Reviewing customer challenge rates for online transactions can uncover fraud and customer experience issues. In addition, marketplace retailers are likely to track defect rates, where a transaction goes bad and a buyer reports a negative experience as this could indicate a latent fraud issue with the seller.

Monitoring websites for unusual behavior is table stakes in the digital world. In particular, retailers may monitor the website sign-in failure rate to identify activity at sign-in or registration that is indicative of a volumetric fraud attack. The mass compromise of login credentials at sites such as LinkedIn and Yahoo are providing criminals with the tools they need to identify vulnerable e-commerce accounts.

“We tend to lose in the fraud landscape as the savings aren’t often significant enough, which is why we have played with all these other KPIs. We unfortunately haven’t gotten it right just yet.”
- Fraud Exec, Marketplace Retailer
Criminals take lists of stolen credentials and leverage automated scripts that will attempt each user name and password at an online retailer’s site in the hopes that a portion can provide access to customers’ accounts.

Fraud management is not naturally a core element of a retailer’s business. Instead, retailers are focused on creating a positive customer experience and building customer loyalty around their brand. That said, finding the right metrics requires insightful fraud staff and a leadership team that empowers them, knowing that ineffective fraud management can undermine the very elements that are central to the success of their business.

Factors That Drive Change in KPIs

As with all metrics, what gets measured gets done. The more confidence senior leadership has in its fraud management metrics, the more likely it can be influenced by them — buying into positive performance and respecting challenges, ultimately leading to the support that fraud teams need.

The most important attribute of a KPI for merchants is that it reduces the array of fraud data that analysts monitor daily to a single point that can be understood and acted on by leadership that does not require the same level of detailed understanding as the fraud team. This necessitates using financial metrics that easily grab attention, such as fraud as a percentage of sales.

Consistent use of the same metric allows senior leadership to view it as a barometer of the current state of fraud management compared with historical data. Layering in industry benchmarks can also prove effective in spurring senior leadership to act, as it could give them a competitive edge over their peers.
Communicating With Leadership

Retailers’ processes for collecting and communicating KPIs will be at varying stages of maturity. The goal for retailers should be to provide senior leadership with easily understood, timely fraud data that allows them to make well-informed business decisions. Achieving the optimal state requires senior leadership’s focus, time, and faith in the value of these processes. Discussions with a multichannel retailer and a marketplace retailer illustrate two varying levels of maturity:

**Mature: Multichannel Retailer**
- Leverage their fraud analytics teams to pull out the fraud trends by store and by product.
- Dig deeper into the data to tease out more underlying details where necessary. That level of detail is not shared with the executives, only a general description of what is being seen and the remediation steps being taken.
- Have more resources to make capital investments in analytics and data mining. This gives them an advantage over smaller retailers in analyzing and preventing fraud losses and covering the losses that get through.
- Communicate weekly with their executives about fraud events.
  - More serious fraud events are escalated immediately.
  - All retailers are challenged in rapidly identifying fraud because of the charge-back process, which can take up to 60 days. Private-label transaction frauds are shared more rapidly.
- When severe fraud events occur, the retailer will initiate communication through conference calls, email notifications with the losses thus far, overall exposure, and the underlying driver.

**Developing: Marketplace Retailer**
- KPIs continue to evolve:
  - Simplifying reporting for leadership in general
  - Adjusting for changing fraud trends
  - Developing new metrics that are deemed more important by leadership.

“I tell my analysts, “You are going to need to put these numbers in plain English for the CFO – try again.”
- Fraud Exec, Multichannel Retailer
Hold monthly meetings to review fraud KPIs. However, there are challenges when there is executive turnover in the fraud department.

Underinvestment in fraud management and the inherent delay from chargebacks contribute to a reactive environment. A fraud event is usually followed by a flood of communication from customers, which makes its way to leadership then back to the fraud team. From there a rapid response workflow is developed and put into place.

**Working With Information Security**

Compared to FIs and issuers, large retailer fraud teams tend to work closely with their peers in information security to identify and manage security events that contribute to fraud. For some retailers, cooperation takes the form of a monthly meeting, where information is exchanged on things like chatter on underground forums that could provide clues about new fraud targets and schemes.

A clear opportunity for cooperation is in leveraging information security to monitor for post-breach activity and subsequently to identify at-risk logins. An example provided by a multichannel retailer involved identifying dormant customer accounts with Yahoo email addresses after the Yahoo breach, which in turn resulted in additional monitoring of these accounts along with closer scrutiny during transactions. As an alternative, the information security team of a marketplace retailer monitored for potentially breached customer logins detected on the dark web and shared them with the fraud team for additional fraud monitoring. With such a significant reliance on the online channel, partnership between fraud and information security teams is a vital element of a successful fraud management program for retailers.
Influencing Investment Decisions

For merchants with exposure to online and mobile channels, fraud as a percentage of sales in these channels can be a significant inducement to invest in fraud prevention solutions. From a fraud loss liability perspective, most of their risk is in these channels and that risk is only growing.

Retailers tend to view fraud as a cost of doing business, especially as fraud may not be detected until months after it has occurred. If fraud losses are within tolerance, then the focus remains on selling and serving their customers. Significant changes to a retailer’s budgeted fraud plan, on the other hand, may motivate research to determine if other retailers are experiencing a similar trend. The results of this research can lead to engagement with vendors, starting with a request for proposals, followed by a pilot and an analysis to determine the systemic impact of the solution before full implementation. There are many providers in the online fraud space, and this process allows the retailer to cut through the noise to find solutions that provide the best return on investment (ROI).

But even among retailers that conduct business in the same channels, there can be unique considerations that motivate investment in certain solutions. Marketplace retailers have more at risk than traditional online merchants, as they can be held responsible for both the cost of lost merchandise and the seller’s fees. With such a wide array of merchandise, these retailers are attractive fraud targets. At the same time, they may eschew onerous fraud controls as they compete with a diverse array of retailers, meaning they cannot risk creating an unpleasant experience as the customer could easily go elsewhere. According to one executive, this has left them without strong authentication at login, resulting in an outsized risk of suffering credential-stuffing attacks using traditional usernames and passwords. The potential for fraud losses and reputational damage has made the sign-in failure rate a critical KPI for this retailer and has led to investments to protect customers’ logins without a sufficiently clear ROI.

“...if our fraud rate is increasing through the online channel we will go out with an RFI to see what others are doing, then we ask for bids from vendors to show us the savings.”

- Fraud Exec, Multichannel Retailer
CONCLUSION

Optimizing fraud management is predicated on effective communication with senior leadership. To achieve this end, FI and retailer fraud teams need to develop an understanding of what leadership deems to be important, translating that into metrics and communication practices that resonate. As fraud continues to evolve, the ability to relay how fraud is affecting the business is critical for securing funding for fraud prevention tools to preserve customer loyalty and company profitability before significant damage is done.

Recommendations

Use metrics that can be easily understood without a background in fraud. The KPIs favored by executives include losses, expenses, and customer impact. The biggest trick is determining what each of these buckets consists of and keeping track of each line item behind the numbers. For example, do expenses include time spent by customer service or information security to research and resolve fraud issues? When the bottom-line numbers change, you’ll need to explain the reasons for the changes. Having this underlying data enables the fraud team to manage changes in their business. The underlying data can be used to put together effective business cases for investments to reduce fraud and demonstrate ongoing fraud solution performance (or lack thereof).

Put a formal process in place for communicating sudden, major events. Don’t wait for the quarterly review to notify leadership of a problem. The leadership team likely has an escalation process in place for other business issues — follow that process as closely as possible. This may include a weekly meeting where high-priority issues are discussed with the right people. Work with the leadership team to understand the types and severity of events they want to be notified about. Each organization will be different in their expectations, so start by leaning toward providing more information and then pare back until the proper balance is achieved.
Don’t just report on what is happening; come to the table with a plan to remediate. The fraud management team owns the fraud problems. Be prepared for the discussion with senior leadership by coming to the table with two or three ways to deal with the problem and the consequences of each option.

Work hand in hand with information security to identify which metrics are leading indicators of potential fraud risk. Daily contact between the groups is a must. It is also worthwhile to cross-pollinate analysts across teams so they know whom to call for different types of questions and indicator sharing. Combining the information security team’s technical knowledge with the fraud team’s view of criminals’ behavior is invaluable.
ABOUT JAVELIN

Javelin Strategy & Research, a Greenwich Associates LLC company, is a research-based advisory firm that advises its clients to make smarter business decisions in a digital financial world. Our analysts offer unbiased, actionable insights and unearth opportunities that help financial institutions, government entities, payment companies, merchants, and other technology providers sustainably increase profits.

Authors: Al Pascual, Senior Vice President, Research Director and Head of Fraud & Security
Kyle Marchini, Analyst, Fraud & Security
Mike Urban, Senior Adviser
Sarah Miller, Senior Analyst – Custom Research & Operations

ABOUT RSA

RSA offers business-driven security solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud, and cybercrime. RSA protects millions of users around the world, and helps 94% of the Fortune 500 companies thrive in an uncertain, high risk world. For more information, go to www.rsa.com.

METHODOLOGY

In support of this study, Javelin Strategy & Research interviewed executives across two industries: financial services and retail. Within financial services, which included digital, regional and card issuing FIs, all institutions were within the top 25 in deposits or number of credit cards in circulation. Among retailers interviewed, which included multi-channel and marketplace retailers, 2016 annual revenue was at least $1 billion.