Web Threat Detection
Trends in E-Commerce
A Guide to Improve Fraud Detection and Investigation
Introduction and Summary

Cybercriminals follow the money wherever it goes. In the case of retailers, the risk/reward ratio is substantial with e-commerce sales projected to eclipse $3.5 trillion globally within the next five years. In addition, the introduction of EMV technology in the U.S. has caused much concern for card-not-present fraud which is expected to hit over $7 billion by 2020.

Another concern for retailers is the threat of account takeover as a result of password breaches. Over three billion user accounts across many popular websites were compromised in 2016, and with the practice of password reuse so common among consumers, retailers are open to the risk of credential replay attacks that result in fraud.

There are many key questions to ask when it comes to how modern cyber threats are impacting global e-commerce including:

- How is cyber fraud affecting retail businesses?
- How prepared are retailers to address the rising tide of online fraud?
- How do retail businesses keep more of their revenue without accepting online fraud as a cost of doing business?

To examine these dynamics more conclusively and to help calibrate expectations on behalf of retailers who compete in this increasingly challenging environment, RSA recently partnered with Gatepoint Research to examine the top issues retailers face when it comes to detecting and investigating fraud and cyber threats. Among the key findings:

Finding the source of fraud takes too long. 72% of respondents reported it takes days or longer to determine the inception point of fraudulent activity on their website.

An inverse relationship exists between the amount of fraud occurring and the size of the teams assigned to investigate it. In fact, 82% of retailers reveal their online fraud investigation team numbers fewer than ten full-time employees, this as one in four retailers cite fraud losses from their e-commerce business as “highly significant.”

Web behavior analytics is new territory for fraud investigation. Only 17% of respondents report being familiar with how web behavior analytics can be used to drastically improve fraud investigation.

---

1 eMarketer
The Most Distressing Impacts of a Cyber Attack

Customers are the key to a successful business. Besides exceptional service and ease of use, consumers want to feel that their information is secure when they conduct business online. Retailers are well aware of the importance of trust as the loss of customer data is clearly the most worrisome security threat.

- **Customer data**: 76%
- **Unexpected downtime**: 69%
- **Fraudulent payments**: 52%
- **DDoS attacks**: 44%
Finding the Source of Fraud Takes Too Long

The lack of insight into fraud and cyber threats ripples across organizations, impacting internal stakeholders and customers alike. It’s an outcome that is familiar to most businesses that suffer a cyber attack but only discover it when the damage is already done.

Over 70% of respondents stated it takes days — or longer — to investigate the origin of fraudulent activity on their website. This is significant as a delay in discovery only serves to lengthen the time cybercriminals have to exploit websites, steal customer credentials, initiate fraudulent purchases and transfers, and perform other illicit activity.

The most concerning outcome? One in five respondents were not even sure how long it took them to discover fraud on their website, which, of course, is highly dependent on just when it was first (if it was ever) detected.

1 in 3 retailers consider it a “major challenge” to detect fraud and suspicious activity across their Web and mobile applications.

72% of retailers take days – or longer – to identify the source of fraudulent activity on their website.
Fraud Investigation: Big Job, Small Team

An inverse relationship of resources to theft opportunities appears to favor cybercriminals rather than the team employed to stop or at least slow them down long enough to mitigate their presence. Even the best threat detection tools won’t help if fraud response teams are not enabled to act fast.

Case Study
A leading retailer was suffering from account takeover fraud as a result of phishing attacks targeted at their customers. Web behavior analytics allowed the organization to detect logins originating from phishing sites, act on a high number of login requests, catch simultaneous access from multiple IP addresses, and alert anti-fraud teams to unusual shopping patterns with discount coupons. With increased visibility into the entire transaction session, the retailer was able to start acting on fraud attempts in hours, not weeks or months.

82% of retailers state their fraud investigation team has fewer than ten FTEs

1 in 4 retailers cite fraud losses from their e-commerce business as “highly significant”
Cybercriminals Take Vacations Too

Cybercriminals are human too, and like us, they pay their bills, take vacations, go to the movies, and appreciate the latest electronic gadgets. The only difference is that cybercriminals seek to use someone else’s hard earned cash or credit to pay their way. Some retailers are more lucrative to cybercriminals, thus potentially hold greater fraud risk.
Web Behavior Analytics is New Territory for Fraud Investigation

Retailers employ many technologies to protect their customer-facing applications, mainly web application firewalls, intrusion detection/prevention systems, web vulnerability scanners, and encryption/tokenization. This polyglot of solutions reflects both the diverse sources of cyber theft and the evolving means businesses are taking on multiple fronts to identify and eliminate threats. However, these legacy tools are not architected to isolate patterns from threats such as account takeover, fraudulent transactions, abuse of business rules, or the scraping of private data off ‘protected’ web pages.

Web behavior analytics is new territory for fraud investigation. In fact, only 17% of respondents report being familiar with how web behavior analytics can be used to drastically improve fraud investigation. But it is rapidly gaining attention for its ability to identify suspicious behavior patterns outside what is typical for a majority of visitors to a website. For example, how do users navigate the site from page to page? Does it comport to other “normal” user sessions around the same time? Are the user’s page transitions, click-times and frequency of clicks by page outside what’s normally observed? By isolating variances, web behavior analytics can interpret and project them to demonstrate that some level of fraud may be occurring.

“Web behavior analytics by its very nature lends itself to quantifiable intelligence on website security. We believe the ability to guide anti-fraud capabilities with business rules, compute risk scores to automate decision-making, and measure the bottom-line effectiveness of anti-fraud mechanisms make a compelling case for organizations to enhance their website protection.”

451 RESEARCH PATHFINDER REPORT: RSA WEB THREAT DETECTION, OCTOBER 2016
RSA Web Threat Detection

RSA Web Threat Detection leverages web behavior analytics to help organizations transform how they detect and investigate digital fraud across their Web and mobile applications. The solution delivers immediate value with an out-of-the-box rules library to address many common high-impact fraud threats, and custom rules can be deployed in seconds allowing organizations to respond in near real-time to emerging fraud.

Today, RSA Web Threat Detection is used to protect many of the world’s leading e-commerce websites and nearly half a billion consumers.

Ask yourself:

• Are you aware of who or what is on your website?
• Are you prepared to act at the speed of fraud?
• Are you ready to take a new approach to fraud risk management?

To learn more about how RSA Web Threat Detection can help, visit www.rsa.com.
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

Copyright © 2017 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA, February 2017. E-book Web Threat Detection Trends in E-Commerce