BUSINESS-DRIVEN SECURITY THWARTS FRAUD IN DIGITAL CHANNELS

BETTER VISIBILITY IDENTIFIES FRAUDSTERS AMONG CONSUMERS

OVERVIEW

It's never been easier to become a fraudster.

In recent years, fraud software vendors have been marketing commercial crimeware used for fraud. In addition, fraud-as-a-service software vendors have been working hard to eliminate technical and financial barriers for new fraudsters. With more user-friendly interfaces, dark vendors are reducing the time between tool acquisition and attack launch. For example, these vendors are selling inexpensive phishing kits, tools that exploit specific security weaknesses, and anti-forensic tools, sometimes conveniently delivered as a cloud service.

The result is a highly-profitable, growing fraud industry. In fact, some analysts claim that the level of fraud automation and sophistication rivals some Fortune 500 companies.

While any organization with an active consumer-facing digital channel is impacted, organizations that are managing multiple web and mobile channels face unprecedented security challenges to prevent fraud without disrupting the user experience of genuine consumers. This impacts many industries including financial services, healthcare, retail, and e-commerce.

As one could guess, with a fraud landscape that continues to grow and change, organizations targeted by fraudsters often have a hard time distinguishing in real-time between legitimate consumers and cybercriminals. Many don't have the tools or visibility to identify fraud activity fast enough to prevent it; often fraud is only noticed after the losses have already occurred. Losses can be dramatic and security teams find themselves unable to answer questions from business leaders about the nature of attacks, the exposure of the organization to these attacks, and the overall business impact. We call the disconnect that exists between these teams the "Gap of Grief".

At RSA, we believe the answer lies in building a new partnership between the security and anti-fraud teams and business leaders in the C Suite and on the Board of Directors. It begins with a layered approach to security that delivers insightful analytics to use as a starting point for discussing security risks in terms of business impact. At RSA, we call this Business-Driven Security™.

THE FRAUD THREAT LANDSCAPE IS CHANGING

To be effective, anti-fraud strategies must be adapted to consider how the fraud threat landscape is changing.

- It is harder than ever to distinguish legitimate consumers from cyber criminals because fraudsters are very good at making fraudulent behavior look legitimate.
- The threat landscape continues to evolve. Fraudsters are more sophisticated and the proliferation of user-friendly tools for fraud has significantly lowered barriers to entry.

- The attack surface is expanding. Consumers are shopping and banking from web browsers and mobile apps, from laptops and mobile devices. And consumers are increasingly using alternative payment methods such as digital wallets.

- Policy management and decisioning is less contextualized because of a lack of visibility into online behavior both before and after the point of authentication.

- Consumers expect both security and convenience and are looking for a frictionless login experience. They are intolerant to any interruptions such as repeated reauthorization.

- Consumers expect to have access to their online accounts 24x7 across all digital channels.

- The costs of investigating fraud are rising as the volume of fraud increases and as attacks become more sophisticated.

- Organizations are unable to align security strategy and activities with risk tolerance and business priorities.

EASIER TARGETS DRAW FRAUDSTER ATTENTION

Let's take a closer look at some areas where fraud pressure is growing:

- **Mobile fraud.** Fraud in the mobile channel has outpaced that of the Web. In 2016, RSA found that 55% of fraud transactions originated from the mobile channel, with 80% of confirmed fraud transactions originating from a mobile app. Organizations face the challenge of increasing mobile security while maintaining a frictionless consumer experience. Therefore, organizations are looking for new authentication features that will be acceptable to consumers, including risk-based authentication, biometrics such as fingerprints and eye scans, and the ability to step up authentication based on transaction risk.

- **Card-Not-Present Fraud.** Analysts predict that as more in-person transactions are secured by the EMV chips that have been embedded in credit and debit cards, fraudsters will increasingly shift activity online. Card-not-present fraud is expected to exceed $7.2 billion by 2020. (See *3-D Secure: The Force for CNP Fraud Prevention Awakens, Aite.*) Let's keep in mind that these are direct financial losses. This puts more pressure on digital channels to better secure cardless transactions. The 2016 release of the 3D Secure 2.0 standard for payment technologies came at a perfect time, with recommendations that offer convenient protection for cardholders. With a focus on the consumer experience, these standards have reduced merchant fears that security measures would increase the rate of abandoned shopping carts. (See *3D Secure 2.0—The New Sheriff in Town*, *RSA.*)

- **Account takeover.** Fraudsters are increasingly attempting to open unauthorized accounts and take ownership of existing accounts. In fact, more than 3 billion user accounts were compromised in breaches in 2016, according to HaveIBeenPwned.com. Automated credential verification tools are making it easier than ever for fraudsters to check the validity of hundreds or thousands of username/password pairs in a few moments. For instance, a popular tool SentryMBA, allows a fraudster to check a list of compromised accounts, identify digital targets, and tailor the way each target is approached and checked. (See *Credential Checking Services Soar in Popularity on Dark Web*, *RSA.*) The success rate of this credential-stuffing is about 5% which means that if a million sets of credentials are tested, 50,000 will be successfully hijacked.

ANTI-FRAUD EFFORTS DO NOT ALWAYS YIELD DESIRED RESULTS

Web and mobile fraud impacts every online business. But while fraud may be a common experience, it isn't an easy problem to solve. In many cases, today's anti-fraud efforts are not working.

- The number of fraud investigators is typically not scaled to the volume of fraud occurring. In fact, 82% of retailers reveal their online fraud investigation team numbers fewer than 10 full-time employees, although one in four retailers cite fraud losses from their e-commerce business as "highly significant."

- Finding the source of fraud typically takes too long. In an RSA survey, 72% of respondents reported it takes days or longer to determine the inception point of fraudulent website activity.

- Threat prevention solutions that don't examine consumer behavior may focus primarily on two points in time: login and transaction. This leads to less contextualized and less informed policy management and decision making. Installing a gatekeeper at a few individual points in the web session is no longer good enough. The entire consumer online user lifecycle must be considered.

- Many solutions lack a mechanism to correlate detected fraud across digital channels and across siloed anti-fraud solutions.

- Many solutions don't do a good job of distinguishing between legitimate consumers and cyber criminals engaging in the same types of online activities (e.g., account access, transactions). Therefore, fraud is often reported by the consumer instead of the merchant, which can delay reporting by weeks.

- Many organizations have implemented point solutions, each of which solves a specific problem. Each point solution becomes an isolated security silo, which makes having a comprehensive fraud and risk management strategy across an entire organization impossible.

- Many organizations can't put fraud details in business context fast enough to prioritize fraud cases based on the business impact. Organizations can't answer simple business questions in the event of fraud: How bad is it? Is it part of a larger pattern? Is it a precursor to a bigger incident? How impactful is this to the business and to the brand?

- Organizations struggle with a lack of confidence and control.

BUSINESS-DRIVEN FRAUD PREVENTION STRATEGY

Legacy anti-fraud tools cannot adequately protect organizations from the onslaught of new and evolving fraud threats. It's time for a new approach that leverages the strength of partnership between technical and business leaders.

Business-Driven fraud prevention provides a layered model to protect consumer identities and assets across multiple channels while allowing organizations to balance risk, costs, and consumer convenience.

Delivering excellent early detection and response services is a start, but Business-Driven fraud prevention technology must also deliver insights that inspire business conversations about fraud threats.

A frictionless consumer experience	A fluid user experience for consumers that allows legitimate users to conduct business while blocking fraudulent transactions. Because advanced features filter out most fraud, stepped up authentication is used for only 3 to 5% of consumer login attempts.
The complete picture	Comprehensive visibility across the entire consumer digital environment, including all digital channels and all user sessions. Visibility also means understanding fraud activity within the context of global, cross-industry threats; for example, fraud intelligence feeds can tell an organization if an IP address or account has been involved in confirmed fraud or if a shipping or email address has been used for mule or fraudulent reshipping activities.
The power of speed and insight	Faster time to insight is fueled by multi-channel analytics and detection capabilities as well as central management of fraud detection, prevention, and mitigation.
Knowledge of business impact	An understanding of business context around a given fraud incident helps business and security leaders manage risk according to an organization's risk tolerance and strategic priorities.
Translate risk policy into action	Faster, decisive response is possible because anti-fraud teams can apply flexible controls appropriate to the level of risk.
Link fraud strategy to business priorities	High-level, dashboard-style reports help organizations see how fraud strategies and activities link to business strategies and priorities.

CONSIDERATIONS IN SELECTING FRAUD PREVENTION SOLUTIONS

Organizations must consider several key factors when considering consumer authentication and fraud detection solutions:

1. Does the solution offer protection beyond login?

2. Does the solution support multiple channels?

3. Does the solution provide flexible policies that enable the appropriate controls to be applied based on the level of risk?

4. Does the solution support multiple options for step-up authentication?

5. How does the solution perform on fraud detection, false positives and consumer challenge rates?

6. Does the solution enable inputs from business intelligence and other anti-fraud tools to be considered as part of the risk assessment?

7. Does the solution assist anti-fraud teams to discuss security risk in terms of business impact?

OUR APPROACH TO FRAUD PREVENTION

The RSA® Fraud & Risk Intelligence Suite is a centralized fraud detection and mitigation platform that uniquely blends continuous monitoring, risk-based decisioning, and fraud intelligence. The Suite combines machine-learning, behavioral analytics, and flexible, rules-based policy management.

A key to the Suite's success is our proprietary approach to layering. The Suite applies various fraud and security controls at each interaction between consumers and a site so that anomalous activity that goes unnoticed by one control can be detected by another control. This approach is highly effective at detecting fraud that otherwise would remain hidden. The Fraud and Risk Intelligence Suite offers:

- Web threat detection.
- Interception and takedown of targeted threats.
- Secure consumer access with multiple approaches to authentication.
- Proven results.

BEST PRACTICES FOR CREATING A BUSINESS-DRIVEN FRAUD STRATEGY

Tools alone aren't enough. A modern fraud strategy requires connecting security risk and business risk that is contextual and specific to the organization. This requires a new way of thinking. RSA has developed best practices and solutions that organizations can use to create a Business-Driven fraud strategy.

- Educate fraud investigators and anti-fraud teams about business impacts and train them to look at fraud from a business perspective.
- Relay important fraud information to business leaders using statistics that are relevant to them in language that they understand
- Prioritize assets and understand their vulnerabilities – e.g., are there different levels of accounts that need to be protected? Can bad actors breach the network through a web or mobile channel?
- Quantify business risk and impact if those assets and accounts were compromised. Consider reputational damage and the associated revenue impact from lost consumers.
- Determine gaps between what is in place today and the ideal anti-fraud state. Take a phased approach to addressing gaps, but start today.
- Build a strategy to defend those assets and accounts that have clear cost/benefit relationships. Prioritize anti-fraud activities according to impact on risk posture, organizational policies, consumer segmentation, and compliance.
- Make sure the organization's fraud strategy is holistic and considers people, processes, and technology. Collaborate to define measurable success criteria and metrics. Define how to calculate Return on Investment by comparing the cost of new fraud prevention investments to savings such as reduced expenses for fraud investigation and reduced fraud losses or improved results such as a better consumer experience.
- Constantly re-evaluate threats and vulnerabilities to fine tune the strategy.
- Have a response plan in place for major fraud incidents.

CONCLUSION

In years past, fraud was viewed primarily as a technology problem, but those days are fading fast. Smart organizations are now viewing anti-fraud efforts through the lens of business impact and prioritizing the security of those things the business values most. This includes protecting the sales revenue stream and delivering a secure and frictionless online experience for consumers.

The RSA Fraud & Risk Intelligence Suite is designed for organizations that want to align fraud prevention efforts with risk tolerance and strategic priorities. The Suite provides a comprehensive view across an environment and across digital channels to clearly see what users are doing on a website or mobile app at any time.

The RSA Fraud & Risk Intelligence Suite also empowers organizations to keep pace with an evolving fraud landscape with features such as self-learning capabilities, customizable behavioral rules that detect and stop fraudsters in real-time, and the ability to digest large quantities of intelligence data from many sources.

With a Business-Driven approach to fraud prevention, anti-fraud leaders are better equipped to discuss the business impact of fraud risk. Then business leaders can work more collaboratively with anti-fraud leaders to ensure that organizations are protecting what matters most.

BUSINESS-DRIVEN SECURITY SOLUTIONS FROM RSA

RSA is a leader in advanced cybersecurity solutions delivering Business-Driven Security™ so organizations of all sizes can take command of their evolving security posture in this uncertain, high-risk world.

Our solutions and services uniquely link business context with security incidents so organizations can reduce risk and be sure they are protecting what matters most.

More specifically, RSA is the ONLY company that enables the three most critical elements of a sound security strategy: rapid response and detection, control at the user access level, and business risk management. No other company does this.

The **RSA® Fraud & Risk Intelligence Suite** is a centralized fraud prevention platform that uniquely blends continuous monitoring, risk-based authentication and fraud intelligence to deliver rapid insight into cybercrime attacks. Leveraging data from your business and other anti-fraud tools, the RSA Fraud & Risk Intelligence Suite enables organizations to greatly improve detection and response to fraud incidents across digital channels without impacting the customer experience.

The **RSA® SecurID® Suite** enables organizations of all sizes to accelerate their business while minimizing identity risk and delivering convenient and secure access to the modern workforce. The RSA SecurID Suite leverages risk analytics and context-based awareness to ensure the right individuals have the right access, from anywhere and any device.

The **RSA® NetWitness® Suite** is a threat detection and response platform that allows security teams to detect and understand the full scope of a compromise by leveraging logs, packets, endpoints, and threat intelligence. By aligning business context to security risks, RSA NetWitness Suite provides the most advanced technology to analyze, prioritize, and investigate threats making security analysts more effective and efficient.

The **RSA® Archer® Suite** empowers organizations to manage multiple dimensions of risk with solutions built on industry standards and best practices on one configurable, integrated software platform.

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 more than 90% of the Fortune 500 companies thrive in an uncertain, high-risk world. For more information, go to rsa.com.

RSA
www.RSA.com