SOLUTION BRIEF

MANAGING RISKS IN CONSUMER FACING DIGITAL CHANNELS

RSA FRAUD & RISK INTELLIGENCE SUITE

OVERVIEW

The consumer world is at a historical inflection point as individuals are interacting and transacting in more ways than we have ever seen. Organizations are going through digital transformations, exposing more and more digital channels to their consumers in order to meet consumer demand for convenience. In turn, this leads organizations to face unprecedented business and security risks ranging from legislative pressure to competition from new entrants to an increase in potential vulnerabilities that can be exploited by fraudsters and cybercriminals.

These changes in the consumer space are impacting different types of organizations, from healthcare to insurance to merchants, and especially financial institutions who are facing massive disruptions such as:

- **Customer expectations for convenience and speed are growing**—customers are expecting to be able to access information from any device, at any time, and execute digital transactions in a fast, frictionless, personalized, channel-agnostic and secure manner.
- **FinTech innovation** is leading to new competition offering digital services, forcing organizations to rethink their strategy and create new partnerships powered by the API economy but also introducing third party risks that must be managed.
- **Sweeping global regulations** are driving more accountability for consumer data protection, security and privacy such as **PSD2**, **GDPR**, **SEPA** and **FFIEC**.
- **Payment innovations** such as **EMV 3D-Secure**, which is expected to drive more merchant traffic through the 3DS ecosystem, "**Faster Payments**" (in its different shapes and forms across the globe), crowd payment applications and

RSA FRAUD & RISK INTELLIGENCE SUITE

- ***Inspire confidence** without inconvenience*
- ***Reduce fraud,** not customers or revenues*
- ***Expose risk** of every digital interaction*
- ***Optimize insight** with collective intelligence*
- ***Enhance efficiency** of fraud operations*
- ***Outpace cybercrime***

other FinTech applications are catalyzing a dramatic growth in the volume of digital payments. As such, the total value of money that is being transferred through digital channels is increasing, exposing organizations to more potential fraud losses.

- The Internet of Things (**IoT**), that enables different devices to perform different activities on the consumer's behalf (take *Alexa* as an example) and as a result the identity of the account holder is practically gone, yet organizations need to be able to differentiate a genuine digital interaction from a fraudulent one.
- Potential points of compromise and vulnerabilities are continuing to expand as organizations role out their **omnichannel strategies**. While each new channel provides more efficiency and streamlined access to financials, it also creates potential security vulnerabilities.
- **Dramatic growth in digital activities and transaction volumes** are offset with minimal (or no) growth in organizational resources to mitigate and investigate fraud. This might lead fraud teams to have **case-marking fatigue**, when the caseload becomes too big for the already overwhelmed analyst team to address. This is a dangerous outcome, as analysts struggle to understand which cases matter most and what should get prioritized. This lack of visibility to identify fraudulent activity fast enough to prevent it can cause fraud to go unnoticed after the losses have already occurred. Losses can be dramatic, and security teams may 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.

This growth in consumer digital interactions with the organization introduces opportunities to grow the organization's revenues, however, it also increases the potential points of compromise and vulnerabilities. The inability to identify digital fraud attempts in real time, in effect, the inability to distinguish between legitimate site users and cybercriminals, can have dramatic consequences for today's organizations – thus, proper planning is necessary. Online fraud reduces revenue by billions of dollars annually in both direct and indirect financial losses including brand damage, which further impacts an organization's ability to attract and retain customers. Fraudsters are increasingly attempting to open unauthorized accounts and take ownership of existing accounts.

As a result, organizations need the ability to identify fraud in real time along with the controls to stop it in real time. They need a comprehensive view of what users are doing in their digital channels at all times so that malicious user behavior, like account takeover and fraudulent money movement, can be exposed. However, they also need the ability to respond to fraud incidents in a way that aligns with their risk tolerance, resources and strategic priorities.

Despite most organizations utilizing over a half a dozen independent anti-fraud tools, each of which solves a specific problem, many organizations lack the ability to correlate them. The need to correlate data from the different anti-fraud tools in order to improve the overall fraud detection rates across all channels as well as to centralize case management will only increase as organizations execute on their omnichannel strategies.

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

BUSINESS-DRIVEN OMNICHANNEL FRAUD MANGEMENT 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, omnichannel fraud management provides a layered model to protect consumer access and transactions across digital channels while allowing organizations to balance revenues, risk, costs, and consumer convenience.

The core of a Business-Driven omnichannel fraud management strategy is an accurate translation of the desired business outcome. Fraud and security teams must understand the business objectives and each decision must align with a desired business outcome.

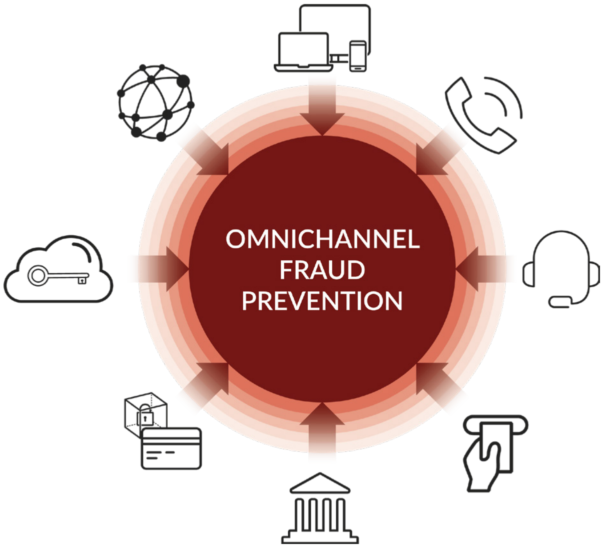

Diagram 1: Omnichannel Fraud Prevention

Establishing simple KPIs such as revenue goals, transaction abandonment rates, customer intervention, fraud detection rates or fraud loss prevention is a start. When these KPIs are established by business leadership, the fraud management teams are able to build and execute a business-driven fraud management strategy by:

- **Setting the right balance between consumer experience in the digital channels and the risk of fraud losses.** Today's users demand fast, easy access to accounts, products, and services in their digital channels and do not want their experience interrupted. Any successful Business-Driven Fraud Management strategy must balance an organization's security requirements with the need for convenient user access and a frictionless user experience.

- **Choosing the right consumer authentication methods.** This can also be critical as there is no "one authentication fits all" model. Organizations should offer a variety of different authentication methods that are convenient to use in different digital channels. Businesses should seek methods that are accurate, with low false positives and low false negatives, as this directly impacts the consumer experience on one hand and the fraud prevention rates on the other hand. Providing a frictionless end user experience to the majority of the organization's end users is a key for customer satisfaction. As consumers are expecting to be able to digitally interact with the organization at any time from any device in a secure and convenient way, failing to meet these expectations might lead to an increase in transaction abandonment rates or loss of customers to competitors, which in turn leads to a decrease in the organization's revenues.
- **Accurately assessing the risk associated with consumer digital interaction.** This is critical for deciding which user can be transparently authenticated and which should be asked for additional authentication. A highly accurate Risk Based Authentication solution with high fraud detection rates and low false positives is essential to meet this goal.
- Verifying they have **full visibility to the way consumers are interacting across all of their digital channels.** This is especially important as organizations seek to open more digital channels through which their consumers may interact. Fraudsters will look for the weakest link and will attack channels that are less secured. Organizations should seek out solutions that provide them with the visibility and insight into how consumers are behaving in their digital channels to be able to accurately differentiate a fraudster from a genuine user.
- Realizing that they cannot fight fraud alone. To be successful in fraud prevention and mitigation, organizations should **collaborate and share intelligence on confirmed fraudulent activities** that will help prevent a fraudulent attack with similar attributes in other organization. The power of a community that fights fraud together can reduce fraud losses significantly.

RSA BUSINESS-DRIVEN OMNICHANNEL FRAUD MANAGEMENT SOLUTIONS

The RSA Fraud & Risk Intelligence Suite is designed for organizations that want to align fraud prevention efforts with risk tolerance and strategic priorities so they can reduce fraud – not their customer base. The Suite provides a comprehensive view across digital channels with a centralized fraud detection and mitigation strategy that uniquely blends risk-based decisioning, predictive analytics, deep entity profiling, flexible rules-based policy management and shared global fraud intelligence, along with the ability to incorporate insight from other anti-fraud tools to enrich fraud risk assessments and better protect customers against targeted cybercrime attacks.

The Suite exposes fraud that otherwise would remain hidden by analyzing each interaction between end users and the digital channel. In addition, the RSA Fraud & Risk Intelligence Suite supports risk-based decisioning at key points during the session such as logins and transactions. The self-learning risk engine conducts deep entity profiling and calculates a risk score that reflects the probability that the activity is performed by a fraudster.

The RSA Fraud and Risk Intelligence Suite protects every step of the consumer digital journey:

- **RSA FraudAction™** is a single external threat management service that offers attack takedown and cyber intelligence. From detection to swift shutdown, RSA FraudAction 360 provides complete coverage against phishing attacks, Trojan attacks, rogue mobile apps and rogue social media pages. The FraudAction Cyber Intelligence Service provides extensive visibility into the cybercrime landscape and operation as it pertains to your brands, leveraging its long-standing, deep visibility into the dark web, combined with deep research within social media forums.
- **RSA Adaptive Authentication** is an advanced, omnichannel fraud detection hub that provides risk-based, multi-factor authentication for organizations seeking to protect their consumers from fraud across digital channels. Powered by the RSA Risk Engine, RSA Adaptive Authentication is designed to measure the risk associated with a user's login and post-login activities by evaluating a variety of risk indicators. Using powerful machine learning, in company with options for fine-grained policy controls, the RSA Adaptive Authentication anti-fraud hub only requires additional assurance, such as out-of-band authentication, for scenarios that are high risk and/or violate rules established by an organization. This methodology provides transparent authentication for the majority of the users, ensuring a frictionless end user experience and high fraud detection rates.
- **RSA Adaptive Authentication for eCommerce** is RSA's EMV 3-D Secure solution for credit card issuers and issuing processors. Utilizing the 3-D Secure protocol and infrastructure, Adaptive Authentication for eCommerce enables merchants and issuers to provide a consistent, secure online shopping experience for cardholders while mitigating the risk of chargeback losses. Powered by RSA's Risk Engine, RSA Adaptive Authentication for eCommerce provides a frictionless shopping experience by silently authenticating good cardholders while challenging only the minority of end users who are high-risk. Its ability to accurately challenge and eliminate fraud while providing good customers with a frictionless shopping experience is unmatched in the industry.

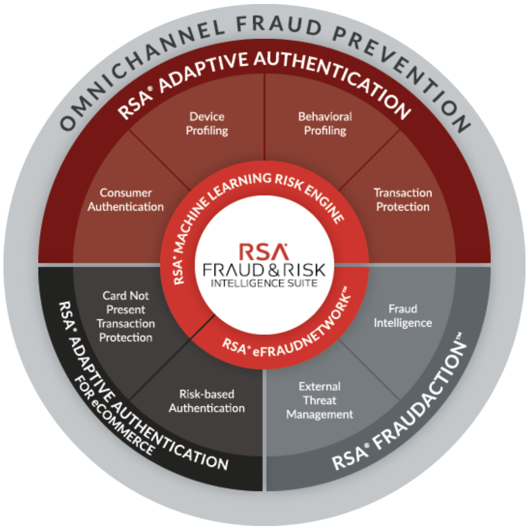
OMNICHANNEL FRAUD PREVENTION
RSA® ADAPTIVE AUTHENTICATION
Device Profiling
Behavioral Profiling
Consumer Authentication
Transaction Protection
RSA® MACHINE LEARNING RISK ENGINE
RSA
FRAUD&RISK
INTELLIGENCE SUITE
RSA® eFRAUDNETWORK™
Card Not Present Transaction Protection
Fraud Intelligence
Risk-based Authentication
External Threat Management
RSA® ADAPTIVE AUTHENTICATION FOR eCOMMERCE
RSA® FRAUDACTION™

Diagram 2: RSA Fraud & Risk Intelligence Suite - Securing the Digital Consumer Lifecycle

PROVEN CONSUMER FRAUD PREVENTION

- ***Over 2 billion** consumers protected*
- ***Over $4 billion** fraud losses prevented a year*
- ***Over 1 million** cyber attacks shutdown*
- ***Over 95% fraud detection** rate with only **3-5% intervention** rate*

***Thousands** of direct and indirect customers **contributing** daily to **RSA eFraudNetwork** - a community that fights fraud together*

RSA Fraud & Risk Intelligence Suite integrates siloed capabilities and data sources to provide a holistic view of individual user activities and behaviors. This cross-product pollination delivers more accurate fraud detection and the ability to craft a highly granular and personalized anti-fraud strategy that aligns with your organization's risk tolerance and strategic priorities.

There are numerous points of integration across the solutions in the RSA Fraud & Risk Intelligence Suite, including:

- **RSA eFraudNetwork™** – the world's first and largest repository of confirmed fraud data elements that are shared between the RSA Fraud & Risk Intelligence customer community. Leveraging data shared within the eFraudNetwork, customers can quickly uncover new types of fraudulent activities and prevent fraud in their environment, based on confirmed fraud shared by their peers.
- **The RSA Adaptive Authentication Eco System approach** is designed to enhance fraud detection by using data elements from different sources. By utilizing third-party facts to influence the risk assessment and impact the risk score, customers can contribute additional insights from both internal business intelligence and additional anti-fraud tools. These days, over 50% of organizations are utilizing between 4 and 10 different anti-fraud tools in their fraud prevention operation. Utilizing the Adaptive Authentication Eco System approach can help organizations to leverage their existing investment in different anti-fraud tools while centralizing the risk assessment and case management in Adaptive Authentication in order to reduce operational cost and increase fraud detection.

Leveraging the integrated RSA Fraud & Risk Intelligence solutions can provide better visibility to your organization's digital channels and help your organization detect and mitigate fraud—both faster and more efficiently.

RSA Fraud & Risk Intelligence Suite delivers holistic omnichannel fraud detection and mitigation capabilities, so organizations can thrive and continuously adapt to transformational change and consumers' ever-increasing demand for convenience while reducing fraud losses and operational costs.

With a business-driven approach to fraud prevention, anti-fraud leaders are better equipped to discuss the current business impact of fraud risks and prepare for the future by enabling them to work more collaboratively with business leaders to ensure they are protecting what matters most to their organization—stopping fraud, not their customers.

DIGITAL RISK IS EVERYONE’S BUSINESS, HELPING YOU MANAGE IT IS OURS

RSA offers business-driven security products and services that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA can help you effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at rsa.com