RSA® Adaptive Authentication
For ecommerce
Risk-based 3D Secure for Credit Card Issuers

SOLUTION BRIEF
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
<tr>
<td>Defining the “New Normal”</td>
<td>4</td>
</tr>
<tr>
<td>The Security Balancing Act</td>
<td>4</td>
</tr>
<tr>
<td>Risky Business: Risk-Based Authentication</td>
<td>5</td>
</tr>
<tr>
<td>Stepping Up to the Step-Up Authentication Plate</td>
<td>6</td>
</tr>
<tr>
<td>Conclusion</td>
<td>7</td>
</tr>
<tr>
<td>Intelligence Driven Fraud Prevention Solutions from RSA</td>
<td>7</td>
</tr>
<tr>
<td>RSA FraudAction™</td>
<td>7</td>
</tr>
<tr>
<td>RSA Web Threat Detection</td>
<td>8</td>
</tr>
<tr>
<td>RSA Adaptive Authentication</td>
<td>8</td>
</tr>
<tr>
<td>RSA Adaptive Authentication for eCommerce</td>
<td>9</td>
</tr>
</tbody>
</table>
The Threat of eCommerce Fraud

eCommerce fraud is a threat to both issuers and merchants, who are targeted by increasingly sophisticated and elusive fraudsters

– Continued roll-out of EMV chip cards will push even more fraud to the online channel as has been seen in countries who have already moved to the chip and PIN cards

– LexisNexis reports that in 2015 large e-commerce merchants saw a 64% increase in revenue losses to fraud year over year. For mobile commerce merchants, year over year revenue loss to fraud grew 24%*

– Merchants adoption is increasing globally - the 3D Secure 2.0 protocol currently in development should drive even more adoption by putting more control of the cardholder experience in the hands of the merchant

– Consumers are concerned with security while on-line, but they want to be authenticated in an nonintrusive manner**

RSA Adaptive Authentication For eCommerce

RSA Adaptive Authentication for eCommerce provides the solution for financial institutions needing to offer additional cardholder protection and fraud management tools for the online shopping experience. Leveraging the widely accepted 3D Secure protocol and infrastructure, it enables merchants and issuers to provide a consistent, secure online shopping experience for cardholders while mitigating the risk of chargeback losses.

Powered by the RSA Risk Engine, RSA Adaptive Authentication for eCommerce evaluates each on-line transaction in real-time to evaluate the level of risk. The RSA Risk Engine analyzes over one hundred indicators per transaction to identify the risk level of the transaction. The Risk Engine’s high level of accuracy drives a very high fraud detection rate along with very low false positive rate.

---

**RSA 2014 Consumer & Privacy Report
AA for eComm can significantly reduce fraud losses while challenging few legitimate customers. Not only does this improve cardholder experience and protect issuer revenue, it drives down operations costs associated with reviewing transactions that are genuine.

**Transparent Authentication for a Frictionless Cardholder Experience**

Utilizing the 3D 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.

RSA Adaptive Authentication for eCommerce allows issuing banks to provide Verified by Visa® (VbV), MasterCard SecureCode, and American Express SafeKey support without impacting their cardholders’ online experience. Using the RSA Risk Engine, Adaptive Authentication for eCommerce transparently evaluates each transaction in real-time and determines the probability that the transaction is fraudulent.

Only cardholders engaging in transactions determined to be high-risk will be challenged to authenticate, leaving approximately 95% of transactions from participating merchants unimpeded by the 3D Secure verification process. In addition, because of the transparent layer of authentication, cardholders are no longer required to go through a VbV, SecureCode or SafeKey enrollment process (the issuer enrolls entire BIN ranges) or remember a password (a range of step up authentication methods including One Time Password are available). This leaves cardholders to transact online uninterrupted.

**The RSA AA For eCommerce Risk Engine**

**The RSA Risk Engine**

The RSA® Risk Engine drives Adaptive Authentication for eCommerce’s industry leading fraud detection rates and low false positives. The Risk Engine performs data mining and identifies new as well as existing fraud patterns by analyzing accumulated customer and transaction data, (e.g., merchant, country code, amount, velocity, device “fingerprints”, user agent, IP address/geo-location and more), as well as behavioral parameters (e.g., user responses to the RSA 3D Secure process) and input from the RSA eFraudNetwork™. AA for eCommerce customers have reported up to an 80% reduction in fraud, driven by the Risk Engine’s accuracy and reliability.
Risk Indicators

Pre-defined indicators are used to alert the RSA Risk Engine of any specific, activity-related parameters known to be risky. The lists of pre-defined indicators are constantly updated using the vast amount of information provided to the RSA Risk Engine and feedback from the issuer’s analysis teams’ and investigation of the Repudiation (Chargeback) files.

Pre-defined indicators include, but are not limited to:
- eFraudNetwork matches of risky IPs, devices, etc.
- Transaction amounts (maximum)
- Behavioral sequences
- High-risk IPs and geo-locations
- Merchants (specific or type)

Profile-driven indicators are used to detect anomalies related to the specific profile and include:
- Device identification & characteristics
- ISPs, countries, connection types
- Velocity anomalies
- Usual activity time anomalies
- Average/cumulative activity amounts
- Previous behavioral sequences

RSA Risk Engine profiling is not limited to the user level; the system also profiles:
- Resources (e.g. IP proxies, devices)
- Combinations of users and resources (e.g. users' browsers)
- User groups (e.g. all users sharing a common profile attribute). Utilizing user groups is one of the many ways that allows the RSA Risk Engine to provide a risk decision even when little historical information is available on a specific user.

Pattern Recognition Analytics

The pattern recognition algorithm consolidates the various parameters and calculates the risk of fraud. The RSA Risk Engine logic is based on a Bayesian machine-learning algorithm, which is a statistical model used to weigh all evidence to calculate the probability of a transaction being fraudulent or high-risk.

The Bayesian analytical model quickly detects emerging patterns based on a small sample of fraudulent activities. Enhanced learning capabilities, unlike the typical learning cycles of one to three months in neural networks, make this model crucial in the online environment as fraudsters are always adapting to the new security measures deployed by financial institutions by constantly switching targets and improving their means of attack.

The fraud risk calculated by the Bayesian algorithm is recalculated on a daily basis, thus keeping the risk model always up-to-date. Some of the unique elements of the RSA Risk Engine include:

- **Risk management.** RSA analysis teams use cutting-edge data mining technology to detect new fraud patterns within Repudiation files generated and sent to RSA on a weekly or bi-weekly basis. This valuable data is collected and reviewed and then used to set risk management rules to counter even the latest and most advanced fraud methodologies. In addition, the fraud patterns can be cross-referenced against other issuers’ data available in the RSA eFraudNetwork, providing organizations with a holistic approach to fighting fraud.
Active sampling. In order to better recognize new fraud trends without increasing the amount of false positives, the RSA Risk Engine employs a method called active sampling. In related cases where there is a slight suspicion of fraud, the RSA Risk Engine actively flags a small sample of them for further investigation. When these cases are identified as genuine or fraudulent, the RSA Risk Engine automatically fine tunes itself for improved efficiency and accuracy in the future.

Learning from feedback. Fraudsters change their behavior rapidly so it is imperative for a fraud detection solution to offer real-time learning capabilities. RSA Adaptive Authentication for eCommerce detects activities suspected of being fraudulent and assigns them high-risk scores. The riskiest transactions are sent to a real-time Case Management system for review by the issuing institution. The investigation results are then relayed back to the RSA Risk Engine which updates itself accordingly.

The RSA Risk Engine works in both directions to keep the false-positive rate to a minimum. In the same manner confirmed fraud implicates associated transactions, the transactions that are confirmed to be genuine update within the RSA Risk Engine. For example, if a new proxy with highly unusual activities is detected, the RSA Risk Engine assigns it as a high risk of fraud. However, if the investigation shows that these activities are legitimate, this information is relayed back to the RSA Risk Engine. This advanced capability allows the system to evolve and adapt at an unparalleled pace.

Success Metrics

The following results have been seen from issuing institutions who have implemented RSA Adaptive Authentication for eCommerce:

- 50%-85% overall fraud reduction for online card-based transactions
- ~95% transactions transparently authenticated and successfully processed
- 50%-70% fraud prediction accuracy with around a 1:1 false positive ratio (FPR) compared to industry standards of over 20:1 FPR in credit card transactions.
- 12 day average reduction in fraud report time – with AA for eComm suspected fraud can be detected and reported as soon as it happens while customers typically call the bank only after they receive their monthly statement

The importance of charge-back data

The RSA Risk Engine easily adapts to and protects against new fraud patterns emerging over time. The Repudiation file, sent on a weekly or bi-weekly basis, helps RSA fraud analysts fine-tune the RSA Risk Engine rules for each issuer. For example, RSA fraud analysts can identify a fraud pattern typical for a specific merchant in a specific location. The information is relayed back to the RSA Risk Engine that uses this data to update the risk management rules in order to prevent future occurrences of this fraud pattern.

User Authentication Options

RSA understands that each issuer has different risk tolerance, business priorities and cardholder relationships. Therefore we offer a broad range of authentication options. Authentication methods used from the platform include:

On-Card Data Elements: These include Card Expiration Date and Cvv2 Code

Off-Card Data Elements: These are selected by the Issuer and can include Date of Birth, Zip Code, Phone Number, Challenge Questions or other Issuer-Defined Elements
**Out Of Band SMS:** One Time Password Challenging high-risk transactions with an SMS which is sent to the customers mobile phone and the corresponding code is used during the check-out process.

**Knowledge-Based Authentication:** Challenging high-risk transactions with top-of-mind questions only genuine users would know (US and UK only).

**Issuer-Defined Authentication Method:** Issuers can leverage their choice of authentication method as well. For example we are starting to see interest from some existing customers in using biometrics to authenticate.

**Functional Description**

**End User Interface**
In RSA Adaptive Authentication for eCommerce, cardholders are only presented a challenge page for high-risk transactions. Issuers can customize the challenge page to reflect their own look and feel as well as the type of challenge to present to their customers.

**Back Office Tools**

**Policy Manager**
RSA realizes the importance of providing our issuing customers with the ability to manage their own card business(es). To that end, RSA Adaptive Authentication for eCommerce offers our customers a robust Policy Manager to help manage their own business as they see fit. The Policy Manager provides:

- Card brand specific user experience
- Ability to balance case volumes
- A controlled way to manage overall fraud costs by business line
- Priority on how and when business rules will be applied
- “Testing Mode” to analyze potential impact before promoting to production

**Case Management**
RSA Adaptive Authentication for eCommerce contains a highly effective Case Management application for tracking transactions that have been blocked or failed an authentication challenge. The Case Management system presents a clear picture of suspected fraud cases, allowing fraud teams to contact cardholders and check if their card has been compromised. Contacting the cardholders and managing the suspected fraud cases has the following benefits:

- Identifies compromised cards as soon as fraud occurs
- Cardholders perceive this as a proactive, favorable action by their financial institution
- Provides insight on current fraud attacks and methods of operation
- Provides a full record of the investigation of each suspected fraud case
- Provides a constant feed of results back into the system

Optionally, if a card issuing institution would prefer to utilize their own case management system, RSA Adaptive Authentication for eCommerce offers predefined integration options to manage cases that have been blocked or failed additional authentication.

**Analytics**
The Analytics Application provides card issuers leveraging RSA Adaptive Authentication for eCommerce with full visibility into their 3D Secure transaction data. The Analytics Application puts daily and monthly monitoring metrics, fraud detection rates and rule performance data at your fingertips so that you can align the solution with your risk tolerance and business priorities.
The dashboard is populated with reports that
– Visualize and highlight trends and outliers
– Allow you to drill in and out for more or less granular views of the data
– Offer a flexible and dynamic interface for on-the-fly changes
You can also export information from the dashboard into a range of formats that can be consumed by external applications.

Reports available in the analytics application include
– Daily, monthly and quarterly overviews
– Fraud levels by volume, value and basis points
– Fraud distribution by risk score
– Risk score distribution
– Case marking
– Rule analysis
– Merchant reports (summary and ranked by chargeback losses)
– Authentication methods
– Step up authentication failures

The Analytics Application provides you with more insight into your threat landscape so that you can make more informed decisions around policy management rules, risk score thresholds and other configurable variables.

Customer Service
The Customer Service application is a web-based application designed to assist the issuer’s Customer Service personnel in helping cardholders with their various inquiries.