RSA® ADAPTIVE AUTHENTICATION FOR ECOMMERCE

Building a secure framework for eCommerce

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. Based on the widely accepted3D 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.

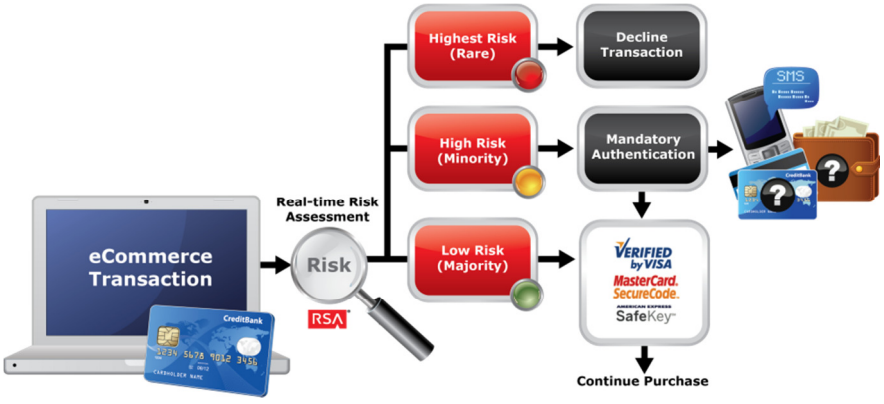
Powered by the field-proven RSA Risk Engine, RSA Adaptive Authentication for eCommerce evaluates each on-line transaction in real-time to evaluate the level of risk. The RSA Risk Engine continually analyzes over one hundred fraud indicators per transaction to assess and determine the associated risk level of a customer and the credit card being used for payment at time of check-out.

HIGH SECURITY WITHOUT COMPROMISING USABILITY

RSA Adaptive Authentication for eCommerce is tailored to handle each and every 3D Secure transaction according to its individual level of risk. Based upon the risk assessment for each transaction a ranking is determined:

- Low-risk transactions (~92-95% of transactions) are transparently authenticated; in most cases, the online shopper is unaware of the authentication process.
- For high-risk transactions (~5-7% of transactions), RSA Adaptive Authentication for eCommerce presents a higher level of security that challenges cardholders to provide additional information to authenticate their identity.

High security without compromising usability means that genuine customers can now freely pass through while fraudsters will be blocked. Thus, the solution can significantly reduce fraud with minimal impact to genuine customers.



THE THREAT OF E-COMMERCE FRAUD

Issuers and merchants are continuously being affected by the threat of e-commerce fraud as they are continually being bombarded from increasingly efficient fraudsters and customers who lack a sense of security while shopping on-line.

- Continued roll-out of EMV enabled cards will push even more fraud to the ecommerce channel as has been seen in countries who have already moved to the PIN enabled cards
- According to Aite, card not present fraud losses will be $3.8B and $6.4B in the U.S. in 2016 & 2018 respectively*
- Merchants now have the flexibility to utilize 3DS based upon check-out "risk" with more & more merchant adoption happening on a global scale
- Consumers are concerned with security while shopping on-line, but they want to be authenticated in an nonintrusive manner**

*Aite, 2014 Issuer & Payment Network Interviews

**RSA 2014 Consumer & Privacy Report

HOW DOES RSA ADAPTIVE AUTHENTICATION FOR ECOMMERCE ESTIMATE RISK?

THE RSA RISK ENGINE

RSA Adaptive Authentication for eCommerce uses the industry proven RSA® Risk Engine to perform data mining and identify new as well as existing fraud patterns. The RSA Risk Engine analyzes 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™ service. As a result, customers using the RSA Risk Engine today have reported up to an 80% reduction in fraud.

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.

RSA

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 provided in the RSA eFraudNetwork, providing financial institutions 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 risk management 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 presented in a real-time Case Management system for further review by the issuing institution. The investigation results are then relayed back to the RSA Risk Engine that updates 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 on-line card based transaction
- ~92%-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 by detecting and reporting suspected fraud 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 can easily adapt and protect 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 Adaptive Authentication for eCommerce supports traditional 3D Secure data elements of authentication such as expiration date, date of birth, or CVV2. Other common forms of authentication methods include:

Knowledge-based authentication – Challenging high-risk transactions with top-of-mind questions only genuine users would know.

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

FUNCTIONAL DESCRIPTION

END USER INTERFACE

The end user interface for RSA Adaptive Authentication for eCommerce will no longer require the Activation During Shopping page. Instead, a challenge page will be presented only 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 additional levels of authentication. 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.

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.

Unregistered cardholders will no longer receive the Receipt page to enter their 3D Secure password. Instead, cardholders will be automatically and transparently authenticated for all transactions—and only challenged to provide additional authentication in the event of a high-risk transaction.

MIGRATING EXISTING 3D SECURE IMPLEMENTATIONS

Customers who have migrated to the most current version of RSA Adaptive Authentication for eCommerce have seen immediate benefits including:

- Average transaction time during check-out is reduced by 45.28 seconds
- Reduced fraud for 3DS related transactions
- Significant reduction in customer service and operational costs
- Higher transaction completion rates with reduced cardholder abandonment

To facilitate the migration, RSA Adaptive Authentication for eCommerce offers an easy path from previous implementations of Verified by Visa, MasterCard SecureCode, or American Express SafeKey. The migration does not require any coding or changes in the existing user interface. Issuers simply need to decide whether or not to cancel registration for their already registered users. An easy utility in the Customer Service application enables financial institutions to cancel registration for specific cardholders. Unregistered cards will be transparently authenticated as if it were a new card in RSA Adaptive Authentication for eCommerce.

Issuers have full control over which cards and users are authenticated with RSA Adaptive Authentication for eCommerce and which cards are authenticated with existing 3D Secure passwords.

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com/rsa.

www.EMC.com/rsa

RSA