RSA® ADAPTIVE AUTHENTICATION FOR eCOMMERCE

Building cardholder protection and fraud management in the online shopping environment

Issuers and merchants can be seriously affected by the threat of e-commerce fraud—not only by actual fraud losses, but the loss of business due to customer concerns in transacting online.

- In 2006, online merchants in the U.S. lost $3 billion due to fraud
- 65% of online shoppers have abandoned a shopping cart/basket or failed to complete an online purchase because they didn't get a sense of security and trust when it came time to provide payment information
- 78% of U.S. online consumers said they are concerned about Internet security when shopping at online sites*

*Forrester Consumer Research

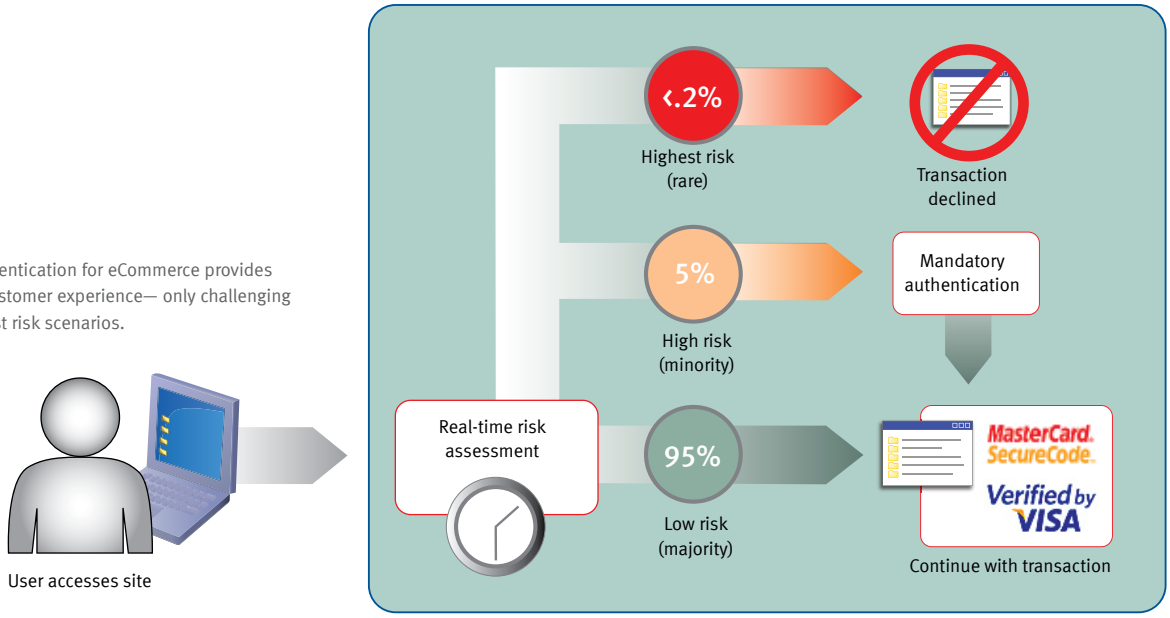
Developed by Visa to provide payment authentication capabilities intended to accelerate the growth of eCommerce through increased consumer confidence and transaction performance, the 3D Secure protocol and infrastructure is today leveraged by more than 125,000 merchants and thousands of issuing banks to provide eCommerce transaction assurance. With recent market trends and negative publicity surrounding online shopping, there is a real demand to find a solution which enables mass adoption, allowing cardholders to shop online with confidence and ease while merchants and issuers can feel assured the transaction is genuine. 3D Secure is in place to create this reality.

However, despite the best efforts of Visa and MasterCard, 3D Secure has established only a limited footprint in North American eCommerce transactions—less than 10%, as of 2007. There are many reasons why 3D Secure has not achieved critical mass despite the urgent market need for such a solution. Some of these fundamental reasons include:

- 3D Secure traditionally requires users to go through an enrollment process and requires cardholders to provide a password during every future transaction. This is reasonable in concept, but reality has shown this process is burdensome and unpopular with cardholders. In addition, it creates significant risk and concern with merchants that customers will abandon a transaction, resulting in lost sales and revenue.
- Issuing banks absorb a liability shift when merchants participate in 3D Secure. 3D Secure has not traditionally included fraud management services, forcing issuers to rely on their existing *card present*-oriented fraud systems to monitor *card not present* fraud. As a result, issuers are absorbing increasing fraud losses from 3D Secure-related traffic which was intended to authenticate transactions to avoid fraud in the first place.

RSA Adaptive Authentication for eCommerce is designed to simultaneously address the issues faced by merchants and issuers while remaining fully reliant on the existing 3D Secure protocol or necessitating any change to authorization streams—creating a complete infrastructure for issuers to permit proper eCommerce transactions for the first time.

RSA Adaptive Authentication for eCommerce provides an unparalleled customer experience— only challenging users in the highest risk scenarios.



ADDRESSING THE NEEDS OF ISSUERS, MERCHANTS AND CARDHOLDERS

RSA Adaptive Authentication for eCommerce provides the framework for financial institutions building cardholder protection and fraud management in the online shopping environment. Based on the 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 charge-back losses.

Used today by more cardholders than any other solution on the market, RSA Adaptive Authentication for eCommerce employs an architecture approved by Visa and MasterCard. Adaptive Authentication for eCommerce leverages the RSA Risk Engine and RSA eFraudNetwork™ service to provide 3D Secure services with native transaction monitoring. RSA provides issuers a single solution to manage their growing fraud losses while creating the shopping experience merchants require to avoid transaction abandonment.

Adaptive Authentication for eCommerce allows issuing banks to provide Verified by Visa® (VbV) and MasterCard SecureCode support without negatively impacting their cardholders' online experience. Using the RSA Risk Engine, Adaptive Authentication for eCommerce transparently evaluates each transaction or activity in real-time to determine the level of risk. Only cardholders engaging in transactions determined to be high-risk will be challenged to provide a secondary method of authentication, leaving 95% of transactions from participating merchants unimpeded by the 3D Secure process. In addition, because of this transparent layer of authentication, cardholders are no longer required to go through a VbV or SecureCode enrollment process, and may conduct commerce online uninterrupted.

BUILDING A SECURE ECOMMERCE FRAMEWORK

RSA Adaptive Authentication for eCommerce is a framework solution providing a multitude of authentication offerings, built on the leading ACS service offering and the market's only integrated transaction monitoring solution.

RSA ACS services

RSA is the world's largest provider of ACS services supporting the largest credit and debit card issuers and processors—including Bank of America, Chase, The Royal Bank of Scotland (RBS) and Lloyds TSB. RSA has extensive experience dealing with even the most complex and demanding requirements as an ACS, ranging from branding schemes to reporting to complex integrations with cardholder databases.

RSA is an all-inclusive, PCI-compliant service provider in an SAS-70 certified hosting environment, allowing issuers to outsource their 3D Secure processing and not require internal development effort. All cardholder user interfaces are developed, maintained, and hosted by RSA, with a rigorous review and approval process in place for issuers to sign off on their cardholder experience. A variety of integration options with cardholder data are also supported, including real-time connectivity and pre-population via batch file.

As part of RSA's flexible authentication framework, numerous data types and authentication schemes are supported. If an issuer requires implementation of traditional 3D Secure authentication schemes, RSA can support virtually any combination of data (such as CVV2, SSN, expiration date, or embossed name) as long as the bank is able to provide access to the information for verification. In addition, RSA's framework can support issuers looking to future authentication schemes including CAP, tokens, or many other common authentication form factors.

RSA Transaction Monitoring services with risk-based authentication

RSA is leading the market today with a transaction monitoring capability natively built into 3D Secure services for fraud detection. Built on RSA's proprietary Risk Engine and leveraging the RSA eFraudNetwork service, Transaction Monitoring utilizes the same technology leveraged within thousands of financial institutions worldwide for online banking and has processed and protected over seven billion online financial transactions to date—an unparalleled base of experience and knowledge in online fraud and risk management.

RSA Risk Engine

The RSA Risk Engine—the core of the Transaction Monitoring service—evaluates each online activity in real-time. The Risk Engine measures over one hundred fraud indicators to determine risk level including

- Transactional parameters (merchant, country code, amount, velocity, device "fingerprints", user agent, IP address / geo-location and additional data),
- Behavioral parameters (user reaction to the 3D Secure process) and
- RSA eFraudNetwork service feeds.

The Risk Engine recognizes anomalies and deviations from pre-defined statistical profiles, and then creates a fraud pattern entry that is added to a data repository of known fraud patterns. Results are produced from day one of deployment without requiring banks to undergo a significant model-building and refining period.

Results-Driven Solution

Based on the results of deployment by a number of large issuers, Adaptive Authentication for eCommerce consistently prevents a majority of 3D Secure-related fraud, with little or no effect on customer usability and lost transactions. The following results demonstrate the efficacy of the Adaptive Authentication for eCommerce solution:

- 50%-85% fraud reduction by basis points
- 50%-70% fraud prediction accuracy—If a transaction is blocked, the likelihood is high that it was indeed fraud (around a 1:1 genuine:false ratio compared to industry standards of over 20:1 in card present transactions).
- 12 day average reduction in time to report fraud—Adaptive Authentication for eCommerce detects and reports suspected fraud in real-time, whereas customers typically call the bank only after they receive their monthly statement.

ABOUT RSA

RSA, The Security Division of EMC, is the premier provider of security, risk and compliance management solutions for business acceleration. RSA helps the world's leading organizations solve their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, encryption & key management, SIEM, data loss prevention, continuous network monitoring, and fraud protection with industry leading eGRC capabilities and robust consulting services, RSA brings visibility and trust to millions of user identities, the transactions that they perform and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

RSA eFraudNetwork: Don't fight fraud alone

The RSA eFraudNetwork is a cross-organization data repository of fraud patterns gleaned from RSA's extensive network of customers, ISPs, and third party contributors across the globe. When a fraud pattern is identified, the fraud data, transaction profile, and device fingerprints are moved to a shared data repository. The eFraudNetwork enables real-time proactive protection to over 100 million online users worldwide that are actively connected to the network and is one of the many sources that feeds the Risk Engine in determining risk.

Risk-based authentication

Adding risk-based authentication to 3D Secure creates a highly effective authentication solution for all parties in the 3D Secure environment. Leveraging the Transaction Monitoring services to evaluate risk, cardholders are only redirected from a merchant site and required to provide extra authentication in the event of a high-risk transaction; only 5% or less of all transactions fall into this category or are automatically issued a declined authentication in the highest-risk cases (less than .5% of transactions). Because cardholders are no longer required to submit to an enrollment process and the majority of transactions are allowed to continue without causing any interruption, Adaptive Authentication for eCommerce provides cardholders with a level of security required to inspire confidence in the online channel and the convenient shopping experience that customers demand.

Self-service applications

RSA provides a full web-based portal of applications supporting Adaptive Authentication for eCommerce, including a detailed Case Management application for reviewing suspected fraudulent transactions. Updated in real-time, the Case Management application is intended to be used by the same internal teams at a financial institution who today reach out to cardholders to review and confirm other suspicious transactions—extending the ability of the issuer to build customer confidence that their card activity is monitored by their issuer and safe to use. In addition to Case Management, RSA includes comprehensive reporting (exportable to Excel), User Administration, and Customer Service applications designed to make 3D Secure fully usable by the business.

h9077-aaecom-sb-0112