

RSA Adaptive Authentication for eCommerce

Reducing fraud losses for credit/debit card issuers while keeping frictionless shopping experience

3-D Secure is an anti-fraud protocol adopted by Mastercard, American Express, Visa, and JCB International that offers another layer of protection to online payments.

The 3-D Secure protocol is evolving. EMVCo, the standards body tasked with developing the new protocol, released the next generation of 3-D Secure in October 2016. The EMV 3-D Secure 2.x protocol seeks to promote a frictionless shopping experience for cardholders by leveraging risk-based authentication technologies—an approach RSA pioneered since 2008.

In the traditional 3-D Secure protocol, each time a cardholder uses a credit or debit card at a participating merchant, that cardholder is authenticated before the transaction can proceed. Authentication in a traditional 3-D Secure environment is based on a password that cardholders create when they enroll their credit cards, and every transaction is challenged.

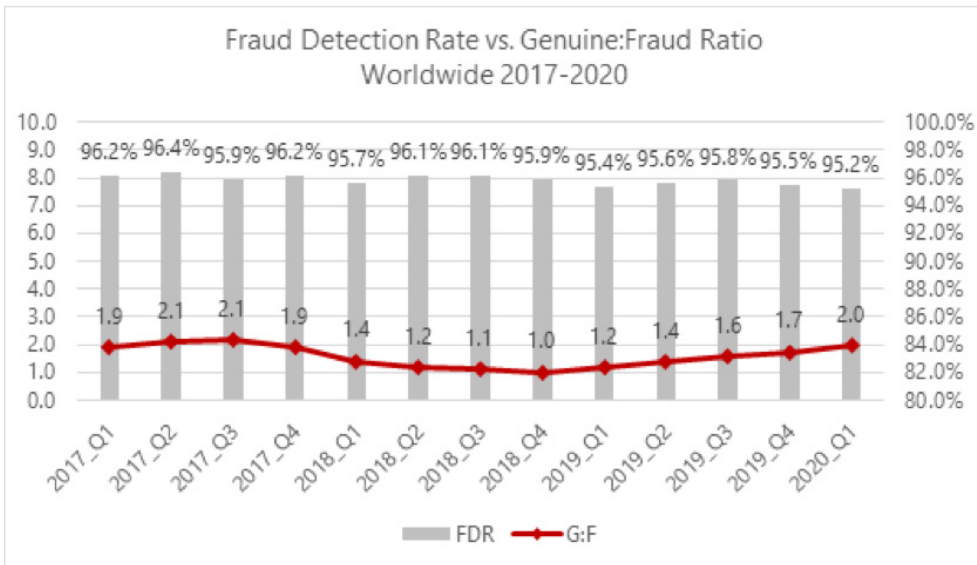
The 100% challenge rate in the legacy 3-D Secure protocol negatively impacts issuers, merchants, and cardholders alike. Any activity that interrupts the purchase flow increases the likelihood of shopping cart abandonment, which reduces revenue for both issuers and merchants. The negative experience created when cardholders forget their passwords also increases the likelihood of cart abandonment, and reduces use of that particular card, further impacting issuer revenue.

The new EMV 3-D Secure 2.x protocol mitigates the negative shopping experience that came along with the legacy 3-D Secure protocol by giving merchants full control over the session. In addition, the new EMV 3-D Secure 2.x protocol suggests a risk-based approach.

RSA Adaptive Authentication for eCommerce has offered a risk-based approach for over a decade and provides high fraud detection rates through strong authentication while eliminating the poor cardholder experience that negatively impacts issuer revenues. With risk-based 3-D Secure, which utilizes machine-learning techniques and anti-fraud expertise, credit and debit card issuers can reduce fraud while protecting revenues.

High fraud detection, low intervention

Adaptive Authentication for eCommerce is RSA's 3-D Secure Access Control Server for credit and debit card issuers and processors. The RSA Risk Engine is at the core of the solution, enabling Adaptive Authentication for eCommerce to silently authenticate cardholders and challenge only high-risk customers (global average of approximately 5% intervention of all transactions). The risk engine's high level of accuracy drives a very high fraud detection rate while maintaining a very low false-positive rate.

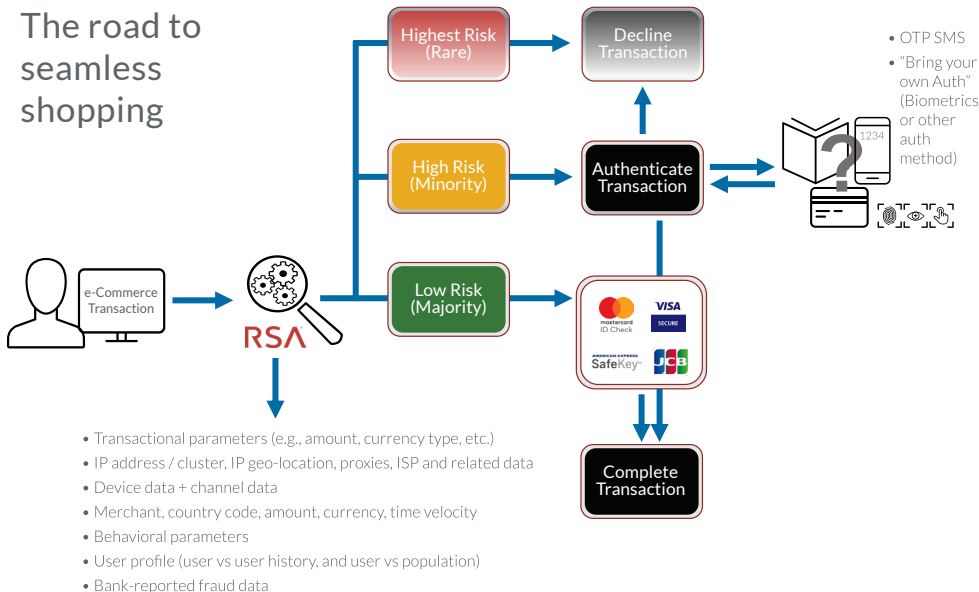


“
The way we measure the success is that we're able to process many more sales, we have our fraud losses under control, and our customers are happy with the solution.
 ”

Vice President and Manager
Fraud Risk Control Large Bank

The graph above shows RSA Adaptive Authentication for eCommerce's average fraud detection rate of 95% and low genuine-to-fraud ratios (i.e., number of genuine transactions challenged for each confirmed fraudulent transaction). RSA Adaptive Authentication for eCommerce can significantly reduce fraud losses while challenging very few legitimate customers. Not only does this improve cardholder experience and protect issuer revenue but it also drives down operations costs associated with reviewing transactions and handling inquiries from genuine customers

Pioneering implementation of new features available with the latest EMV 3-D Secure 2.x protocol, RSA 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 Visa Secure, Mastercard Identity Check, American Express SafeKey and JCB J/Secure™2.0 support without negatively impacting their cardholders' shopping 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 EMV 3-D Secure 2.x verification process. In addition, because of the transparent layer of authentication, cardholders are no longer required to go through a Visa Secure, Mastercard Identity Check, American Express SafeKey or JCB J/Secure™2.0 enrollment process (the issuer enrolls entire card BIN ranges beforehand) or remember a password (a range of step-up authentication methods including one-time password and biometrics are available). This leaves genuine cardholders to transact online uninterrupted.

As an industry pioneer and an EMVCo technical associate, RSA provided feedback to the EMV 3-D Secure 2.x standard, which was reflected in the specifications. RSA Adaptive Authentication for eCommerce enables credit/debit card issuers and processors to leverage the latest functionality as specified by the protocol.

About RSA® Fraud & Risk Intelligence Suite

RSA® Fraud & Risk Intelligence Suite enables organizations to manage risk across consumer-facing digital channels, allowing them to maximize revenues and minimize fraud losses. The suite is part of the RSA portfolio of business-driven security solutions, which provides a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. 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. For more information, go to rsa.com.

