RSA® ADAPTIVE AUTHENTICATION FOR ECOMMERCE

Risk-Based 3D Secure for Credit Card Issuers

3D Secure is an anti-fraud protocol adopted by MasterCard, American Express, Visa and JCB International that offers another layer of protection to online payments. In the 3D Secure protocol, each time a registered cardholder uses an enrolled credit card on a merchant site that participates in 3D Secure, that cardholder is authenticated before the transaction can proceed. Authentication in a traditional 3D Secure environment is based on a password that the cardholder creates when he enrolls his credit card and each transaction is challenged.

The 100% challenge rate in traditional 3D Secure negatively impacts issuers, merchants and cardholders alike. Any activity that interrupts the purchase flow increases the likelihood of 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 even reduced use of that particular credit card, further impacting issuer revenue.

Risk-based 3D Secure offers high fraud detection rates through strong authentication while eliminating the poor cardholder experience that negatively impacts issuer revenues. With risk-based 3D Secure, credit card issuers can reduce fraud and protect revenues.

HIGH FRAUD DETECTION, LOW INTERVENTION

Adaptive Authentication for eCommerce is RSA’s 3D Secure solution for credit card issuers. The RSA Risk Engine is at the core of the solution, enabling AA for eComm to silently authenticate cardholders and challenge only high risk customers (typically ~5% of all transactions). The Risk Engine’s high level of accuracy drives a very high fraud detection rate along with very low false positive rate.
The graph above shows AA for eComm’s average fraud detection rate of close to 95% and low genuine to confirmed fraudulent ratios (i.e., number of genuine transactions challenged for each confirmed fraudulent transaction). 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.

**TRANSARENT 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.

**3D Secure 2.0 – The Next Generation**

The 3D Secure protocol is evolving. EMVCo, the standards body tasked with developing the new protocol, is preparing to release the next generation of 3D Secure (3DS 2.0) in 2016 or 2017. The 3D Secure 2.0 protocol seeks to promote a frictionless shopping experience for cardholders by leveraging risk-based authentication technologies – an approach RSA pioneered in 2008. As an EMVCo Technical Associate, RSA is providing input to 3DS 2.0, input reflected in the protocol as it is taking shape.

RSA looks forward to enabling the new functionality within our platform once 3D Secure 2.0 is officially released. We will continue to work directly with our customers and EMVCo on initiatives that will help card issuers transparently authenticate cardholders within the existing 3DS infrastructure as well as the future versions of the protocol all under the assumption of never using a password.

“...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 for the Fraud Risk Control Division, Large Bank