

The Evolution of 3D Secure:

*Applying New Techniques to an Existing Technology
Can Boost Antifraud Effectiveness*



By Karisse Hendrick, Editor-at-Large, CardNotPresent.com



Online-fraud prevention is a continually moving target. As fraud tools become more sophisticated, fraud tactics and attacks also evolve to find undiscovered vulnerabilities and ways to continue to profit from using stolen credit-card data. While the main focus of a fraud strategy is to protect the bottom-line by canceling fraudulent orders before they result in chargebacks and lost product, there is little guarantee that all those orders would result in chargebacks if not canceled. Companies must ask themselves if they would rather risk more loss for the sake of potential sales, or risk sales for the sake of preventing fraud.

But some companies have found a way to reduce fraud and increase top-line sales. By combining 3D Secure (3DS) with Big Data and what issuers call risk-based authentication (RBA) merchants are able to have more confidence in a transaction and reduce the amount of orders they cancel post-authorization. MasterCard SecureCode and Verified by Visa have been in existence for more than a decade. When these products first launched, however, they were considered difficult for consumers to use and the cause of a high amount of shopping-cart abandonment.

Originally, 3DS asked consumers to enter a bank-supplied password for every enrolled transaction before it could be completed. Consumers were not well educated about the system and, therefore, unprepared for it when making a purchases at participating online businesses. As a result, adoption of 3DS was limited. Since then, however, card brands and issuers along with providers that enable merchants to process 3D Secure messages have worked together to make major changes to this system.

Merchants and issuers now can choose which transactions require the consumer to enter a password, significantly lowering the friction to customers enrolled in the program. Beyond this upgrade, many issuers now are using RBA along with 3DS protocols that allow the issuer to use its history of the consumer's behavior and Big Data analytics to make more educated decisions when authorizing a transaction. It also allows a merchant using 3DS to send additional information about the order to be verified against the issuer's history with the consumer, such as IP address, device ID, mobile phone number, e-mail address, etc. This exchange of information allows an issuer to add more data to their consumer profile while gaining more trust in the merchant's abilities to spot fraud.

“3D Secure with rules-based authentication provides more intelligence than 3D Secure on its own, and allows the merchant to be more in control of the sale, enabling merchants to increase sales while also decreasing fraud,” says Michael Roche, vice president of Consumer Authentication at CardinalCommerce, a technology provider that leans on a decade of accumulated data about consumers and issuer behavior to help merchants select which transactions they will run through 3DS.

The Evolution of 3D Secure:

*Applying New Techniques to an Existing Technology
Can Boost Antifraud Effectiveness*



Visa and MasterCard see so much potential in 3DS they have incentivized merchants and issuers to participate in the program. Every transaction processed through the 3DS protocols is guaranteed against being charged back to the merchant. Along with that liability shift, there is also a significant discount on interchange, ranging from 12 to 59 basis points for every 3DS transaction. CardinalCommerce says it sees an average savings of 19 basis points across all merchants, which also includes a mix of transactions across both card brands and some transactions that were not run through 3DS. Merchants that run their transactions through 3DS can reap these benefits, said Roche, even if they never allow a transaction to be challenged and initiate with issuers who do not participate in 3DS.

Using a strategy to initiate 3DS and RBA at the beginning of its fraud screening process has allowed passenger-train operator Amtrak to be more confident in a bank's decision to authorize or decline a transaction, especially knowing the issuer will accept the fraud liability for that transaction.

“By being strategic in where we initiate 3D Secure in the transactions process, we have seen a large decrease in the orders we were declining due to a suspicion of fraud,” says Rick Ziolkowski, program director of Card Security for Amtrak. “This has led to a significant increase in card acceptance, with no risk of those orders turning into fraud chargebacks.”

The system allows them to be selective about which cards go through enhanced authentication with 3DS, but should an issuer have a track record of high cart abandonment or challenging a significant number of transactions, Amtrak can run them through their legacy systems, to ensure a quality customer experience while still preventing fraud.

“We have seen a sea change in the evolution of fraud prevention,” Ziolkowski adds. “First generation tools like AVS (Address Verification System), CVV2 and others that have been used in the past cause high friction. Customer input errors created a high error rate in declining orders we assumed were fraud. 3D Secure has allowed Amtrak to relax these legacy rules where we now have protection. 3D Secure presents this legacy data to the issuer during authentication, and incorporates additional risk-based authentication data captured during the customer checkout session. The issuer has a deeper relationship with our shared customer by seeing all of their purchase activity across their payment history. We see this as a common sense approach to allow the issuer to make the more accurate decision, and with the liability shift, it's really a no-brainer.”

CardinalCommerce still advises merchants to layer their fraud-prevention tools, and to continue to use a fraud-prevention case management or rules-based system instead of relying solely on their system. The company says the product's best use case is at the beginning of a transaction to leverage the issuer's information with the added security of the liability shift, and to use a standard fraud tool to decision transactions that the issuer does not feel confident in.

The Evolution of 3D Secure:

*Applying New Techniques to an Existing Technology
Can Boost Antifraud Effectiveness*



“We don’t see our product as being used in place of a traditional merchant fraud tool, but as an added layer of protection against fraud,” says Tara Lavelle, vice president of Marketing at Cardinal. “Just like you wouldn’t want to drive a car without both a seatbelt and airbags.”

Using a layered approach leveraging 3DS, merchants can reduce fraud and chargeback losses, decrease interchange processing fees and make fewer unnecessary declines while being selective in how transactions will be routed, for an optimal customer experience. With more governments around the world mandating 3D Secure to secure transactions and reduce the volume of fraud in specific markets, more merchants are getting beyond the stigma of this product to mitigate fraud while increasing revenue.

About CardinalCommerce

CardinalCommerce is the pioneer and global leader in enabling authenticated payment transactions in the card-not-present industry since 1999. With One Connection to their proprietary cloud-based payment platform, Cardinal enables Consumer Authentication and alternative payment services (including digital wallets and mobile commerce). This SafeCloud™ enables friction-free, technology-neutral authentication across a wide range of applications, and allows expansion into new technologies as they develop, so that merchants can securely accept payments from the entire financial transaction ecosystem, without development on their end. For more information, visit www.cardinalcommerce.com.

About CardNotPresent.com

CardNotPresent.com is an independent voice generating original news, information, education and inspiration for and about the companies and people operating in the card-not-present space—one of the only sources of content focused solely on this growing segment of the payments industry. Our only product is information. Our only goal is to provide it in an unbiased manner to our subscribers. The company’s media platforms include the CardNotPresent.com portal, the hub for news, information and analysis about the payments issues that most affect merchants operating in the space; the CNP Report, an e-newsletter delivering that focused information directly to your email inbox twice a week with no extraneous clutter; the CNP Expo, an annual gathering of the leading companies in the space from the smallest e-commerce Websites and technology providers to global retailers and payment processors; and the CNP Awards, an annual event honoring the products and solutions CNP merchants rely on most to increase sales. For more information, visit www.CardNotPresent.com.

© Copyright 2015 CardNotPresent.com. All rights reserved.