VIEWPOINT

April 2020

201 Boston Post Road West, Suite 301 | Marlborough, MA 01752
www.mercatoradvisorygroup.com |phone 1-781-419-1700 |email: info@mercatoradvisorygroup.com

REVISITING AUTHENTICATION IN THE AGE OF SRC AND EMV 3-D SECURE

The time for a new authentication strategy is upon us.

International card networks are mandating issuers worldwide deploy Secure Remote Commerce (SRC) and EMV 3-D Secure (3DS) to increase the security of e-commerce. Issuers must decide if they will update their authentication method to better support cardholders and merchants or continue to utilize a less secure challenge—the password—that is known to drive high cart abandonment. Now is the time to plan a transition away from passwords.

By Tim Sloane, VP, Payments Innovation, and
Director, Emerging Technologies Advisory Service

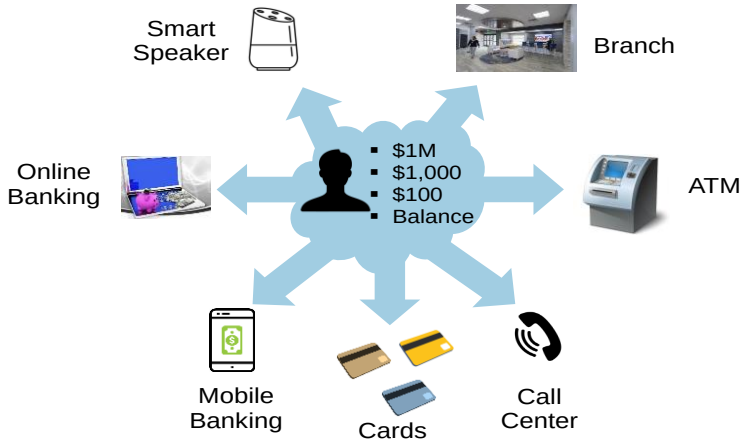
Why Should You Care About SRC or EMV 3-D Secure?

Technology has progressed since we made the following statement in the Mercator Advisory Group research report titled *Biometrics: A New Wrinkle Changes the Authentication Landscape,* in January 2017. With the introduction of the European Union's revised Payments Services Directive (PSD) with its requirement for strong customer authentication (SCA), and with the payment networks' deployment of EMV 3-D Secure (3DS) version 2.2 we are even more confident in the statement's accuracy today.

> Despite their customer data being under attack by criminals who have stolen literally billions of consumer credentials, executives in banks, credit unions, and other financial institutions should carefully review any investments their organizations are making in the deployment of new authentication technology, for which the return on investment requires 3–5 years. Clearly the current authentication schemes have come under withering attack, and this puts bank assets at risk. But the road forward is not well marked, and we are fast approaching what will prove to be a critical fork in that road.
>
> Further securing the traditional two-factor authentication mechanisms utilizing variations of "what you know," and "what you have" increases security but also makes it harder for the rightful owners to access their assets. Biometrics will deliver much greater authentication security while simultaneously making it easier for customers to access their assets by adding "what you are" as a new factor.

Consumers are increasingly trusting and adopting biometrics on the smartphone and are becoming accustomed to using their smart speakers for a range of use cases. Mercator's consumer research indicates that smart speakers are now owned by 60% of the U.S. adult population and over time consumers will want to make payments and access financial services using these devices.

Figure 1: How many authentication methods must a consumer endure?



Source: Mercator Advisory Group

As shown in **Figure 1**, consumers face an increasingly complex authentication landscape that protects their assets differently depending on the channel they utilize. Since it is well recognized that convenience is critical to consumer adoption, it is time for financial institutions to rein in the multiplicity of authentication methods they use to identify account holders and even employees. Using multiple different authentication techniques creates unwanted friction in the effort to protect assets, sometimes taking several seconds for the customer to respond. The lack of an integrated solution results in an inconsistent user interface that not only detracts from the customer experience in doing business with a company but is likely to frustrate the company's digital team's plans for a seamless cross-channel customer experience, which every industry is now attempting to create.

Now consider how EMV 3-D Secure 2.0 will affect cardholders. If every card issuer deploys a different authentication method, then cardholders will be confronted with a different challenge for each card they use. Perhaps one card requires a personal identification number (a PIN), the next requires a password, the next a one-time password (OTP), and another a biometric. The cardholder, driven by muscle memory, comfort, and convenience, is likely to settle on using just one card. If you are an issuer and want that card to be yours, you need to start training your customers now by implementing the same authentication technology across all delivery channels as soon as possible. A customer who uses a biometric to access all of the bank channels shown in **Figure 1** is likely to feel most comfortable using that bank's card which delivers the same experience during the EMV 3-D Secure challenge. Addressing every channel and technology using a different authentication technique is a mistake because it fails to reinforce a common behavior and set consumers' expectations.

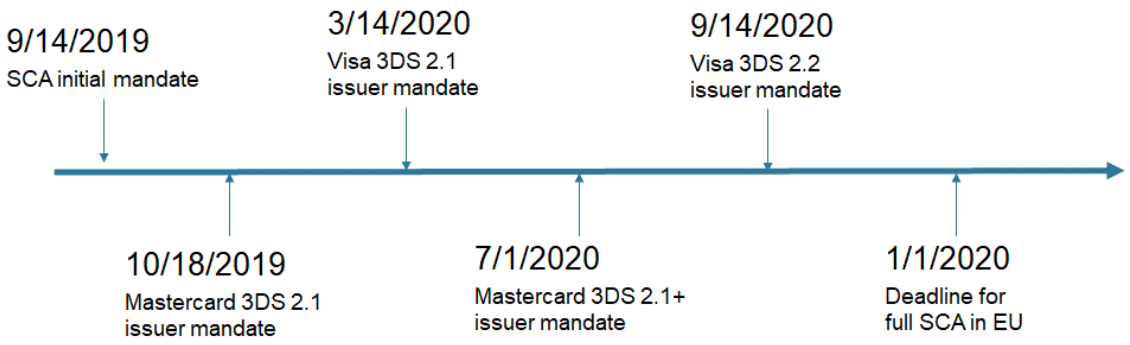
A customer who is presented with the same authentication technique for every interaction with a financial institution becomes more familiar with that technique. This increases the customer's confidence in interactions with the financial institution and reduces the customer's apprehension if confronted with an identical authentication request when shopping online. Although this comfort can be achieved with any common authentication type, the forthcoming Mercator Advisory Group Viewpoint *Biometrics: Consumer Adoption Rates and Sentiment* makes a strong argument that the authentication technique should be implemented on a smartphone, which Mercator consumer research indicates 89% of U.S. adults over the age of 18 already have.

3-D Secure Is More Than You Think

EMV 3-D Secure is needed first and foremost to meet the requirements mandated under PSD2 by the European Union. The E.U. has issued a mandate that all payments that don't fall under a relatively restrictive set of allowed exemptions must adhere to specific consumer authentication standards defined by strong customer authentication (SCA). The dates for remaining compliant under PSD2 are shown in ***Figure 2***.

Meeting the compliance deadlines shown in Figure 2 may seem simple but is actually made complex by the individual network requirements and rules. The rules specify technical requirements, authorization procedures, and liability shifts. For example, Mastercard's October 18, 2019 issuer mandate is a bit misleading. On this date all Mastercard issuers can reject any payment that is submitted without at least EMV 3-D Secure version 1. For merchants to be sure an issuer will not reject an authorization, they will minimally need to support 3DS v1. If the merchant submits an authorization without 3DS v1, the issuer can "step up" the transaction and request the transaction be resubmitted with a minimum of 3DS v1.

Figure 2: The EMV 3D secure dates for PSD2 compliance.



Sources: Ingenico, Ravelin, and Mercator Advisory Group

But don't think 3-D Secure is only for the European Union. It is arriving in the United States, where Mastercard has mandated that issuers adopt 3-D Secure v2 globally by April 1, 2019.

The Visa mandate was adjusted to August 31, 2020 for the United States, Canada, the Asia-Pacific region, Europe, the CEMEA region (Central Europe Middle East and Africa), and LAC (Latin American and the Caribbean). The activation date for EMV 3-D Secure v2 (formerly 3DS 2.0) has been changed to August 31, 2020 for the U.S., Canada, Europe Asia-Pacific, CEMEA, and LAC, to align with other improvements and E.U. requirements.[i]

Note that both Mastercard and Visa networks provide a stand-in service that will respond on behalf of issuers that have not implemented 3-D Secure v2. However, issuers that rely on the stand-in service will bear liability when the merchant submits a 3-D Secure transaction.

More important, EMVCo is extending the role of EMV 3-D Secure authentication beyond just card payments. Future versions are expected to support the provisioning of wallets and tokens as a new method for identification and verification (ID&V) solutions as well as support identification for consumers opening a new account or even support use as a more general user authentication mechanism. It should come as no surprise that Mastercard currently has pilots (in Australia and Macedonia) for identity solutions[ii] and has launched an initiative it calls ID Check that is already being positioned as a method of provisioning mobile devices.[iii] Visa also has a robust authentication strategy under its ID Intelligence offering that includes validating identity documents, biometric authentication, device fingerprinting, and validation of user data.[iv]

Then there are the multiple third parties offering solid solutions for this environment. An example is a solution from Entersekt that implements digital certificates, device fingerprinting, and web-based cryptographic binding technology to establish a unique browser identity. For low-risk transactions, this approach enables customer access with zero friction. As the risk increases, the orchestration layer can implement a step up to smartphone-based authentication through the bank app. If a customer doesn't have the bank app or loses the phone, the solution utilizes an SMS one-time password, out-of-band voice call, or Fast Identity Online (FIDO) to authenticate the individual.

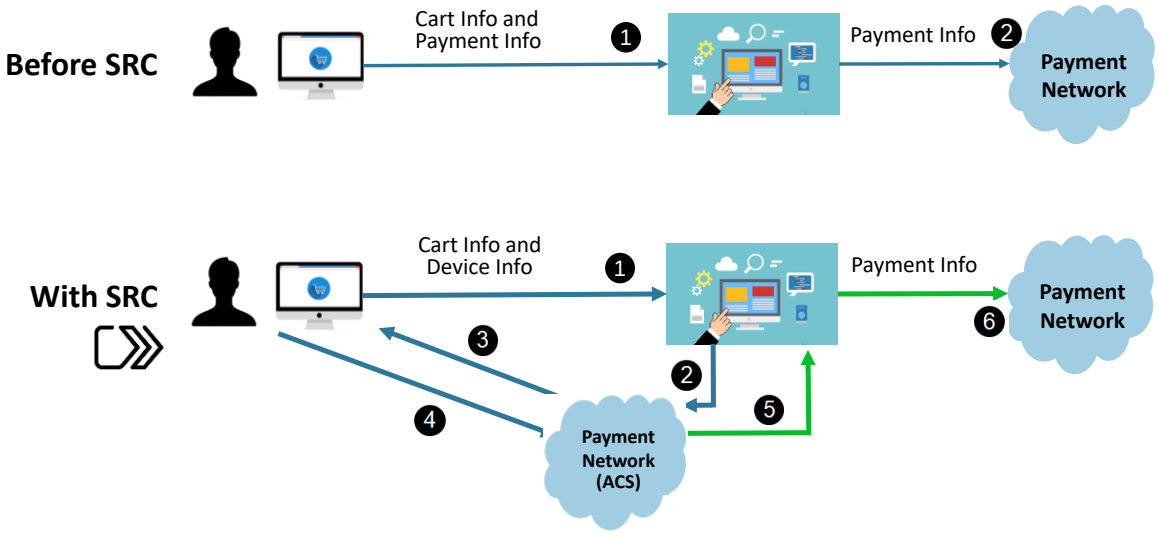
Benefits of a Strong and Consistent Authentication Infrastructure

For a financial institution (FI), there are multiple benefits to consolidating the authentication methods around a one-touch authentication experience. It enables a seamless best-of-breed cross-channel digital experience and improves customer trust and convenience, including a one-touch browser experience. Implementing one-touch authentications can also help the FI protect customers against phishing and other attacks by fraudsters once customers recognize the authentication technique and expect it for every interaction with the FI. As the FI's customers come to trust the digital experience and convenience, they will access the FI's site more often, make more transactions, and gravitate to the FI's card products that share the same authentication method.

Secure Remote Commerce (SRC)

To understand EMVCo's Secure Remote Commerce, let's start by reviewing SRC's benefits and how they are delivered. EMVCo and the payment networks have positioned Secure Remote Commerce, or SRC, as an important mechanism for reducing e-commerce fraud. If widely adopted by merchants, SRC does indeed eliminate several current fraud vectors, including the Magecart malware and other malware that infects checkout screens, because SRC eliminates payment data from the merchant's website. It also eliminates exposure from data lost to hackers because it replaces card data with tokens (unless the merchant requests the card number and other personally identifiable information, or PII). However, the safety SRC delivers does come at a cost to merchants in both time and effort because it requires new code on the user front end as well as the ability to accept payment details via a new secure channel on the back end, as shown in the simplified diagram in ***Figure 3***.

Figure 3: A simplified view of how SRC protects user data.



Source: Mercator Advisory Group

At the top of Figure 3 is the traditional e-commerce website, which presents the consumer with a cart that contains details regarding the products purchased, taxes, shipping, and cost. It also presents the purchase card

network options that the merchant supports, such as American Express, Mastercard, or Visa. The consumer enters payment details, which are sent (1) to the e-commerce site via the web and then passed (2) to the network for authorization. In this model, the payment data, although sent via a secure HTTP session, is ultimately deposited (perhaps by a gateway) into the e-commerce site environment with card data exposed for the merchant to see (and criminals to steal).

The diagram at the bottom of **Figure 3** represents the SRC method. The user can still view the merchant shopping cart with multiple purchase options, but a new icon is also visible. When the user selects the SRC payment method (by clicking on the SRC icon shown at far left in the diagram) the merchant collects the consumer data (1) from the user (including user device data), which is then passed (2) to the Access Control Server (ACS) implemented within the payment networks. The ACS server evaluates the user device data to determine if the user is already enrolled in SRC. If the user is enrolled and passes basic authentication, the user is next presented with a personalized wallet (3) that lists the cards that the user has enrolled in SRC. Note that multiple cards from multiple issuers and card networks can be represented in the wallet but no complete card numbers are exposed, only the image of the card and the last four digits. The user selects a card to use for this transaction, and the selection is communicated to the ACS (4). The ACS then creates and delivers a token using a secure connection to the merchant's system back end (5) (note that a primary account number, or PAN, can be delivered if requested by the merchant). With cart and payment method information in hand, the merchant then decides how it wishes to authorize the transaction (6), which may or may not invoke an EMV 3-D Secure transaction. For readers interested in a more detailed explanation of how SRC operates, see this blog on the Mercator Advisory Group site.

SRC Controversy

The Secure Payments Partnership (SPP) has voiced its displeasure with EMVCo standards in general and SRC specifically. SPP consists of retail groups and payment networks committed to greater security and transparency across the payments system. The SPP founding members include the Food Marketing Institute, National Retail Federation, National Association of Convenience Stores, National Grocers Association, and Shazam, a PIN debit network.

Public complaints made by the Secure Payments Partnership claim EMVCo is not a "true standards body." Mercator agrees with that opinion from the perspective that a traditional standards body by default specifies a standard to assure two different implementations are interoperable. While some standards issued by EMVCo do deliver compatibility and even include certification, such as EMV Cards and EMV Readers, other standards EMVCo has issued are very vague, with details left to the implementer. For example, the tokenization standard left the details associated with interfacing to the token vault almost entirely up to the implementer (details of this are provided in the Mercator research report *Payment Networks 2.0: The Battle for Tokenization*). As a result, interoperability was impossible unless the two implementers agreed to integrate the two solutions together. This happened in late 2016 when Mastercard and Visa announced they would establish interoperability.[v] The interoperability is not an open EMVCo standard, however, but a private function unavailable to other payment networks. If EMVCo is interested in the widest possible adoption of its standards, it would do well to make them more detailed and fully available to interested parties, as other standards bodies do.

EMV 3-D Secure

Once the consumer has decided to buy an item from an e-commerce site, SRC sends the payment information to the merchant via a secure communications channel. At this point, the merchant will utilize whatever payment process it desires, which means that ultimately it will use either EMV 3-D Secure or a traditional authorization mechanism. Within the European Union, if the transaction doesn't fall under a PSD2 exemption, then EMV 3-D Secure will be used to remain compliant with PSD2's requirement for strong customer authentication (SCA), which requires two-factor authentication.

Note that the latest version of EMV 3-D Secure is version 2.2. Differences in versions include the following:

- The initial specification was EMV 3-D Secure 2.0, first published by EMVCo in 2016.
- Version 2.1 introduced frictionless authentication and shorter transaction times, and yet it collects roughly 10 times more data than version 1.0.
- Version 2.2 adds support for exemptions, including acquirer-side transactional risk assessment, low-value transactions, and whitelisting of merchants.
- Future versions are likely to support expended use cases, including identification and verification solutions as used when provisioning a mobile device, when opening a new account, or even used as a more general user authentication mechanism.

Ways for Merchants to Avoid SCA

SCA is not required for a range of exemptions granted by the issuer, and merchants are likely to try hard to take advantage of them:

- Recurring transactions (after the first transaction has been authenticated)
- MOTO transactions (mail/telephone order)
- One-leg-out transactions (where the card is issued or the merchant is based outside the E.U.)
- Direct debits
- Consumers will have the right to "whitelist" trusted businesses, enabling issuers to exempt the transaction from SCA requirements. However, if the issuer establishes the exemption, the issuer also bears the liability for fraud, so issuers may be slow to adopt whitelists.
- Issuers and acquirers may also exempt transactions valued under €500 if they maintain low levels of fraud. This is possible using the exemption within PSD2 called the Transaction Risk Analysis (TRA) exemption, which requires that overall fraud be maintained below the following levels:

  — 0.13% for transactions up to €100

  — 0.06% for transactions up to €250

  — 0.01% for transactions up to €500

- When a transaction is suspicious (as defined by the issuer), the issuer will request SCA even if it falls under an exemption.
- If SCA is required but does not take place, the issuer will "soft decline" the authorization request. This means the transaction was approved after the issuers' risk assessment but the network identifies the transaction as requiring SCA compliance and so performs a soft decline.

Two important points related to processing EMV 3-D Secure transactions. First, every participating issuer should implement a risk-based authorization process. The additional data delivered by the merchant (address, IP, etc.) should be analyzed to help guide the decline or acceptance of the transaction. The definition of risk related to an acceptance decision is left entirely up to the issuer. Importantly, issuers will hold the liability for any fraud on that transaction when authorized with EMV 3-D Secure if the issuer grants an exemption to the merchant or if the issuer hasn't deployed EMV 3DS (and the merchant submits a EMV 3DS transaction). If the exemption is applied by the acquirer, the acquirer owns the liability unless the issuer performs an EMV 3DS challenge on the transaction.

It should also be noted the EMV 3-D Secure is the name for the EMVCo standard. Each brand has deployed this 3-D Secure protocol as a unique product offering with its own name and regulations. The Visa product is Verified by Visa; the Mastercard product is Mastercard SecureCode; the American Express product is SafeKey: and the Discover product is ProtectBuy.

Conclusions

SRC modifies the interaction between the merchant and the cardholder. EMV 3-D Secure 2.0 modifies the interaction between the merchant and the issuer and shifts liability for fraudulent transactions when they are mistakenly approved by the issuer. While SRC and 3-D Secure 2.0 are a priority for the global payment networks, there is controversy regarding how these standards will support the EFT debit networks. Issuers competing for top of wallet need to consider carefully the impact of the way they authorize cardholders making the transactions. Experience with early versions of 3-D Secure made it clear that many cardholders are unlikely to enter passwords when challenged on a merchant e-commerce website. With the volume of e-commerce transactions growing rapidly, especially during the coronavirus pandemic when customers have to "shelter in place," issuers need to rethink how they intend to authenticate cardholders making e-commerce transactions. In Mercator's opinion, issuers need to think beyond authentication of the cardholder. It is time to rethink all authentication methods used in the issuer's financial institution.

In a forthcoming Mercator research report, *Biometrics: Driven by Standardized Authentication, Adopted by Consumers*, we demonstrate the importance of authentication via biometrics on the smartphone. Biometrics are the primary solution being deployed to meet PSD2 requirements for strong customer authentication, or SCA, in the European Union. Use of biometric authentication eliminate the need to send one-time passwords using SMS or email—both of which are recognized as unsafe. But this recommendation extends beyond cards: The financial institution should implement a consistent biometric-enabled authentication process for all channels.

A financial institution's use of a different authentication method for every channel inhibits user confidence and lowers user convenience. Mercator advocates for an authentication implementation strategy that is based on the

smartphone as the common authentication device across all channels. While a smartphone solution can't be deployed to every customer and used on every channel today, it should be the long-term goal. A properly provisioned smartphone becomes the first factor "something the consumer has." The second factor would be a combination of different biometrics and perhaps physical devices (secure key dongles) that can be relied on in different risk scenarios. Checking balances or moving low value might be approved with a behavioral biometric even without a direct user challenge, while higher-risk scenarios would directly challenge the user with a request to implement the smartphone's biometric scan or the presence and confirmation of a physical dongle.

To enable this new authentication model requires that the financial institution move to a risk management model that calibrates the risk associated with each transaction because a biometric isn't deterministic (pass/fail); rather, it is probabilistic. Creating an arbitrary risk limit cutoff that mimics traditional password pass/fail logic could put your institution at greater risk. Mercator recommends every financial institution start to plan its implementation of a consolidated authentication model that is based on risk as soon as possible.

References

Related Research by Mercator Advisory Group

Distributed and Self-Sovereign Identity Solutions: Part 1, Technology Overview (August 2019)

Distributed and Self-Sovereign Identity Solutions: Part 2, Implementations and Suppliers (September 2019)

Securing E-Commerce: Competing Technology Crowds the Market February 2019)

Behavioral Biometrics Will Restructure the Authentication Landscape in the Next 5–8 Years (May 2017)

Biometrics: A Market Forecast for Consumer Adoption (January 2017)

Biometrics: A New Wrinkle Changes the Authentication Landscape (January 2017)

Payment Networks 2.0: The Battle for Tokenization (October 2014)

Endnotes

[i] https://cdn.ingenico.com/binaries/content/gallery/corporate/global-epayments/global-epayments-2020-pages/psd2_webpage_timeline-resized.jpg, accessed 3/29/2020

[ii] https://www.paymentsjournal.com/mastercards-products-for-identity-and-authentication-continue-to-gain-government-adoption/, accessed 2/11/2020

[iii] https://www.mastercard.co.uk/en-gb/consumers/features-benefits/strong-customer-authentication.html, accessed 2/11/2020

[iv] https://developer.visa.com/site/visa-id-intelligence, accessed 2/11/2020

[v] https://usa.visa.com/visa-everywhere/security/secure-digital-payments-through-tokenization.html, accessed 3/27/2020

Copyright Notice

For more information about this report, please contact:

Tim Sloane, VP, Payments Innovation, and Director, Emerging Technologies Advisory Service
tsloane@mercatoradvisorygroup.com
1-781-419-1712

Mercator Advisory Group is the leading independent research and advisory services firm exclusively focused on the payments and banking industries. We deliver a unique blend of services designed to help clients uncover the most lucrative opportunities to maximize revenue growth and contain costs.

Advisory Services. Unparalleled independent and objective analysis in research documents and advice provided by our Credit, Debit and Alternative Products, Prepaid, Merchant Services, Commercial and Enterprise Payments, Emerging Technologies, and Global Payments practices.

Primary Data. *North American PaymentsInsights series* presents eight annual summary reports based on primary data from Mercator Advisory Group's bi-annual surveys of 3,000 U.S. adult consumers to determine their behavior, use, preferences, and adoption of current and emerging payment methods and banking channels to help our clients identify and evaluate business opportunities and make critical business decisions. Two other Mercator survey series—*Small Business PaymentsInsights* and *Buyer PaymentsInsights*—each receive coverage in three reports annually.

Consulting Services. Services enabling clients to gain actionable insights, implement more effective strategies, and accelerate go-to-market plans. Offerings include tailored project-based expertise, customized primary research, go-to-market collateral, market sizing, competitive intelligence, and payments industry training.

PaymentsJournal.com. The industry's only free, analyst-driven, online payments and banking news information portal delivering focused content, expert insights, and timely news.

For additional copies of this report or any questions, contact Mercator Advisory Group at 1-781-419-1700.