Federal Reserve Bank of Boston®

Payment Strategies Report | March 17, 2021

De-Mystifying New Approaches to Safer Online and Mobile Payments

Susan Pandy, Ph.D. and Marianne Crowe, Federal Reserve Bank of Boston

Executive Summary written by David Lott, Federal Reserve Bank of Atlanta

Contents

Marianne Crowe is vice president and Susan Pandy is director in the Payments Strategies Group at the Federal Reserve Bank of Boston. The views expressed in this paper are solely those of the authors and do not reflect official positions of the Federal Reserve Bank of Boston or the Federal Reserve System. David Lott is a payments risk expert in the Retail Payments Risk Forum at the Federal Reserve Bank of Atlanta.

The authors would like to thank members of the MPIW and other industry stakeholders for their engagement and contributions to this report.

Executive Summary

E-commerce sales continue to gain a larger share of overall retail sales – a trend that the U.S. Department of Commerce's quarterly data reports show has existed since 2011. The COVID-19 pandemic, which made many consumers reluctant to shop in person and drove many businesses to close, has accelerated the gain in share since March 2020. Total retail sales in third quarter of 2020 increased 7 percent over third quarter of 2019. E-commerce sales increased 36.7 percent in third quarter of 2020, representing 14.3 percent of retail sales.[1]

Prior to COVID-19, criminal activity focused mainly on card-not-present (CNP)[2] or e-commerce merchants, compared to the physical retail environment. E-commerce has become an even larger target in the present COVID-19 environment, making consumer authentication more critical to combatting fraud. Recognizing the increased risk of this channel, several industry organizations that develop technical specifications have been updating their protocols to improve the security of the e-commerce channel and the consumer purchase experience.

EMVCo[3] published the 3-Domain Secure (EMV®[4] 3DS) protocol and functional specifications in December 2018 and the Secure Remote Commerce Specification v1.0 (EMV SRC or EMV SRC Spec) in June 2019.[5] The World Wide Web Consortium (W3C)[6] introduced the WebAuthn specification (in coordination with the Fast Identity

---

[1] U.S. Census Bureau. (2020, Nov. 19). Quarterly retail e-commerce sales 3rd quarter 2020. U.S. Department of Commerce. https://www2.census.gov/retail/releases/historical/ecomm/20q3.pdf.

[2] Card-not-present (CNP) is a type of payment for a purchase where the card/cardholder are not physically present for the merchant to validate at the time of purchase (e.g., by U.S. postal mail, telephone, or online). Buy online, pickup in-store (BOPIS) and in-store mobile quick response (QR) code transactions are also considered CNP according to card network rules even though the cardholder is physically present for such transactions.

[3] EMVCo is a global technical body that facilitates worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV 3DS specifications and related testing processes (e.g., chip-based payment cards, payment tokenization, and 3DS). American Express, Discover, Visa, MasterCard, JCB, and Union Pay jointly own EMVCo. EMVCo manages and evolves EMV 3DS specifications and testing processes for card and terminal evaluation, security evaluation, and interoperability issues. Membership and voting are primarily held by the card networks. An executive committee comprised of card network representatives provides guidance on long-term strategy, with working groups making decisions on a consensus basis. Associate-level membership is available to industry stakeholders (e.g., financial institutions, processors, merchants, vendors, etc.) to provide input to new specifications. EMVCo does not mandate how its specifications should be implemented. Therefore, readers should not expect EMVCo to discuss implementations. https://www.emvco.com/

[4] EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC. Full information is available at: https://www.emvco.com/wp-content/uploads/2018/05/EMVCo_eBook_FINAL.pdf.

[5] EMVCo (2018, Dec.) *EMV 3-D Secure protocol and core functions specification*. Available at https://www.emvco.com/emv-technologies/3d-secure/. EMVCo (2019, June). *EMV Secure Remote Commerce specifications v1.0*. Available at https://www.emvco.com/emv-technologies/src/.

[6] World Wide Web Consortium (W3C) was established in 1994 as an international community where member organizations, staff, and the public work to develop open Web standards to ensure the long-term growth of the Web. W3C seeks interoperability across browsers and the Web. W3C is decentralized; four institutions host its activities: MIT (Cambridge, MA), ERCIM (Sophia-Antipolis, France), Keio University (Tokyo, Japan), and Beihang University (Beijing, China). It is comprised of more than 60 experts and 444 member organizations.

Online (FIDO) Alliance)[7] and relevant application programming interfaces (APIs) in March 2019. The FIDO Alliance's Client-to-Authenticator Protocol (CTAP) complements WebAuthn; together, the specifications comprise FIDO2.[8]

The Mobile Payments Industry Workgroup (MPIW) formed a subgroup in June 2019 to better understand these specifications and publish their findings in a whitepaper. Along with sub-group calls, the Federal Reserve Bank of Boston Payment Strategies team conducted approximately 15 confidential interviews with industry stakeholders, including card networks, financial institutions (FIs), acquirers, gateways, processors, digital wallet providers, technology providers, merchants, and industry groups. This whitepaper identifies key challenges to adoption and provides industry education and guidance about how the various protocols may complement each other and enhance the security of the online and mobile channels.

Key takeaways include:

Overall

- The online consumer checkout experience remains challenged by inconsistent processes resulting in high shopping cart abandonment rates and inferior customer satisfaction.
- Consumers expect and increasingly demand a fast and secure payment experience, regardless of the channel or device used.
- The specifications represent significant changes to minimize consumer involvement, reduce friction, and increase successful sales transactions (customer conversion).
- The specifications are in early stages of adoption and implementation. Limited documentation of results has created some industry stakeholder reluctance to implement.
- The COVID-19 environment has shifted stakeholder resource priorities, particularly for issuers and merchants.

EMVCo Secure Remote Commerce

- EMV SRC eliminates the need for an enrolled consumer to enter payment credential details for future online transactions.
- Most large issuers support EMV SRC, but only through initial conversion of their card network digital wallet cardholders (e.g., Masterpass, Visa Checkout).

---

[7] FIDO Alliance was launched in 2013 as an industry association focused on authentication standards to help reduce the overreliance on passwords. FIDO Alliance has over 260 members, with membership levels at the board, sponsor, or associate levels. FIDO drives technical progress through workgroups and subgroups at the technical, adoption, and regional levels. Board and sponsor members can participate on the workgroups and subgroups, but associate level members participate by invitation-only.

[8] See https://www.w3.org and https://fidoalliance.org/.

- Acquirers and processors indicate that the card networks are at different stages of maturity in the implementation process, which complicates the stakeholder experience.
- EMV SRC benefits merchants that are moving to the digital environment, have higher proportions of guest checkouts,[9] and use card-on-file (CoF)[10] tokenization.
- Key merchant issues include inability to enroll a co-branded merchant payment card, order of payment cards in the Candidate List,[11] compliant debit routing, and customer experience impact.
- More consumer education is needed to alleviate customer concerns and increase adoption.

EMV 3-Domain Secure (Version 2.2)

- While 3DS 1.0 was widely implemented in the EU due to regulatory mandates, it received poor reception in the U.S. for several reasons, including consumer and FI enrollment requirements and PIN/password entry on pop-up windows.
- EMVCo released EMV 3DS 2.2 (EMV 3DS) in December 2018. The specification supports global interoperability and uses risk-based authentication (RBA)[12] with 10 times the number of data elements working in the background.
- Step-up authentication for consumers will only be required in high-risk transactions and is expected to represent less than 5 percent of a merchant's transactions.
- More coordination among industry stakeholders (issuers, acquirers, processors, and merchants) is needed to create a useful data subset for EMV 3DS transaction messaging.

FIDO Alliance

- The FIDO standard provides issuers with additional information about the authentication method that facilitates their risk decision.
- Many issuers support FIDO authentication when they accept Face ID on Apple devices. Apple authenticates the provided biometric stored in the secure element of the mobile device so issuers can trust this authentication to unlock the issuer's mobile app.

---

[9] Guest checkout refers to the option on a merchant website for a consumer to proceed with a purchase without creating an account with the merchant (e.g., create username, password and share email and other information) or storing payment credentials with the merchant.

[10] Card-on-file (CoF) is the authorized storage of a consumer's payment credentials by a merchant, payment service provider, or wallet service provider so that the consumer can make repeat or automatic purchases without re-entering payment credentials for every transaction.

[11] The Candidate List displays enrolled cardholder payment cards for the cardholder to select to make online payments.

[12] Risk-based authentication (RBA) analyzes hundreds of indicators in real time and forms a dynamic assessment of the level of risk, allowing a decision to be made with a high degree of confidence to allow access to an account. "Kapersky Fraud Prevention." 2021. http://www.kapersky.com/

- FIDO authentication eliminates the need for issuers to rely on one-time password (OTP) authentication methods that create customer friction.
- Card networks benefit from FIDO because a merchant can serve as the FIDO or WebAuthn relying party and leverage EMV 3DS to report FIDO authentication data to the issuer.

W3C

- W3C APIs are building blocks that help web developers create a webpage that works consistently across browsers.
- W3C works to enhance browsers and create a more intuitive user payment experience.
- The Payment Request/Payment Handler APIs are web technology designed to eliminate cumbersome online forms that consumers fill out to make purchases.
- Similar to EMV SRC, W3C APIs can streamline guest checkouts and minimize friction for returning shoppers.
- The WebAuthn/FIDO2 specification is now ubiquitous in the market, as most browsers and mobile phones support it with biometric authenticators.

I. Introduction

Both e-commerce and mobile commerce (m-commerce)[13] sales volume continue to expand rapidly in the U.S. In the first half of 2020, U.S. e-commerce sales reached $371.9 billion. This represents a 30 percent year-over-year increase from the first half of 2019 and more than double of the previous year's growth rate, largely fueled by the impact of COVID-19. The Census Bureau estimates that U.S. retail e-commerce sales for the second quarter of 2020 increased 44.5 percent over the second quarter of 2019. Business Insider Intelligence forecasts that 44 percent of all retail e-commerce will be generated via m-commerce by 2024.[14] Despite historically low customer conversion rates for merchants, stemming from a frustrating checkout process on a small screen, mobile phones are now a driving force behind m-commerce growth.[15] This is, in part, due to streamlined checkout experiences offered by digital wallets optimized for smaller devices. According to eMarketer, 2020 will realize notable increases in both digital buyers and average spending per buyer because of the global pandemic. Whether the consumer uses a mobile application (app), digital wallet, or CoF payment method,[16] the industry needs to provide more customer convenience, as

[13] Mobile commerce, or m-commerce, is the use of wireless handheld devices (e.g., mobile phones, tablets) to conduct commercial transactions online, including, but not limited to, the purchase and sale of products, online banking, and paying bills.

[14] Meola, A. (2019, Dec. 17). Rise of m-commerce: Mobile ecommerce shopping stats & tends in 2020. *Business Insider*. https://www.businessinsider.com/mobile-commerce-shopping-trends-stats.

[15] *Ibid*.

[16] Payment method refers to "buy" buttons (Amazon Pay, Pay with PayPal, Shop Pay), credit, debit, proprietary payment cards, prepaid cards, ACH, mobile/digital wallets, including PayPal and the "Pay"

well as trusted platforms that protect the consumer's identity, payment credentials, and personal information.

The rapid growth in m-commerce has created opportunities for multiple payment options or "buy" buttons. Some industry stakeholders are concerned about fragmentation, while others say it provides more customer choices. Merchants will have to decide what they want for their customers.

EMVCo, FIDO, and W3C have collaborated to develop technical specifications that address stronger authentication and improve online purchase experiences. These organizations have unique perspectives on how to develop specifications. EMVCo focuses on the card payments industry, and W3C focuses on standards to ensure the growth of the web. FIDO's focus is broader than payments and develops standards and certifications for authenticators that are hardware-, mobile-, and biometrics-based, shifting the industry away from usernames and passwords. Other solutions, such as digital wallets, also address online authentication and enhancing the consumer experience, but are not specifically addressed in this whitepaper.

EMVCo published a specification to address the use of digital terminals for online commerce and to streamline the guest checkout process. They introduced the EMV *Secure Remote Commerce Specification v1.0* (EMV SRC) in June 2019 and created the Click to Pay icon in June 2020 (which appears on a merchant's checkout page). EMVCo also published the EMV *3-Domain Secure Protocol and Core Specifications (v. 2.2.0)* (EMV 3DS) in December 2018.

W3C introduced the WebAuthn specification and the Payment Request and Payment Handler application programming interfaces (APIs).[17] The FIDO Alliance worked with W3C on WebAuthn and released the Client-to-Authenticator Protocol (CTAP). These specifications seek to address pain points in the consumer online checkout experience and enhance overall security by reducing fraud.

In 2019, the Mobile Payments Industry Workgroup (MPIW) formed a subgroup to gather information about these specifications, determine their impact on the payments industry, and educate industry stakeholders about the purpose of the protocols. The specifications are at different stages of adoption and implementation, with many unanswered questions. The payments industry needs a more holistic understanding of these specifications.

The objective of the MPIW subgroup was to explain the relationships between the protocols, and help stakeholders make informed decisions about how to best leverage

---

wallets (e.g., Apple Pay, Google Pay, Samsung Pay), buy online/pickup in store, buy now-pay later, and installment payments (e.g., Affirm, Afterpay, Klarna).

[17] An API is a set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service. APIs include protocols and codes that determine how different software components, i.e., programs, can communicate with each other. The developer creates the API on the server and allows the client to talk to it.

the specifications to enhance the security and consumer convenience for online and mobile shopping. They reviewed and assessed the specifications to:

1) Educate the payments ecosystem about what the specifications do, how they differ, overlap and/or complement each other
2) Understand which stakeholders are implementing the specifications, identify use cases, and note specific opportunities, challenges, or gaps in the process
3) Understand how different stakeholders (e.g., issuers, card networks, merchants, acquirers, processors, digital wallets, and consumers) apply the specifications
4) Identify and address industry questions, concerns, and business issues

Part II is an overview of the specifications. Part III discusses stakeholder perspectives for each specification, including perceived benefits and challenges to adoption. Part IV includes key messages and recommendations.

II. Overview of the EMVCo, FIDO, and W3C Specifications

Significant changes are underway in the current global payments environment, in terms of regulation, consumer behavior (particularly in light of the global pandemic), and innovation to enhance security, authentication, and the remote consumer shopping experience. Currently, the average consumer has to manage passwords for more than 70 applications, which the payments industry recognizes as a problem.[18] These technical specifications represent a shift away from reliance on static data elements, such as vulnerable passwords, to more advanced technologies, including biometrics (e.g., fingerprints, facial recognition, behavioral, and technologies included in mobile phones), behavioral analytics, and other strong customer authentication methods that may impact how user and device authentication are managed in the future.

A. EMVCo Secure Remote Commerce (EMV SRC) Specification

EMV SRC is the most recent approach to enable consistent and streamlined processing of e-commerce transactions across digital channels and devices. Implementations began in December 2019.

A general frustration among online shoppers is the need to enter data in multiple fields to complete a purchase.[19] Customers new to a merchant website may need to include personal information, payment card details, billing and shipping addresses,

---

[18] NordPass (2020, Feb. 26). *New research: An average person has more passwords than an average pop song has words*.

[19] This does not include consumers who use payment methods in which they are already enrolled, such as Apple Pay, Google Pay, Samsung Pay, PayPal, Amazon, or merchant proprietary methods. The whitepaper refers to consumers who may not have a preferred payment method that they use frequently; and often resort to guest checkout or manually entering their payment information for each purchase.

email address, and phone number. While this information is critical to the payment and delivery of the purchase, it may increase shopping cart abandonment for merchants that do not offer buy buttons. Requiring a customer to create an account, or presenting a checkout process that is too slow or complicated, contributes to over 40 percent of shopping cart abandonment.[20] Many merchants seek to improve their shopping cart conversion rates (percentage of completed transactions) and offer the customer an easy and convenient checkout process.

EMV SRC creates a consistent consumer experience for online checkout by reducing the need to enter personal data and payment credentials, thereby reducing checkout time and abandonment rates. Similar to a POS terminal payment, the EMV SRC process is the same regardless of the payment card used, but EMV SRC uses a virtual payment terminal in an e-commerce environment. Like digital wallet solutions, EMV SRC securely transmits payment and related checkout data that can further minimize fraud associated with e-commerce websites and mobile apps. EMV SRC improves the guest checkout experience for consumers who do not want to use a digital wallet or create a merchant relationship (online account) and share personal information.

The EMV SRC spec is interoperable with EMV payment tokenization, dynamic data, and EMV 3DS for CNP transactions. Payment tokenization improves authorization approval rates by enabling issuers to collect more data about the token requestor (TR)[21] for a tokenized transaction (e.g., whether it is a merchant with strong fraud management tools) and confirm the known relationship between the cardholder and the TR. Many issuers report higher authorization rates with EMV tokenized transactions.

Understanding Roles, Operations, and Status of EMV SRC

Currently the card networks perform all EMV SRC supporting roles, although the specification allows other entities to assume some roles. They are trying to promote broader industry engagement to achieve large-scale adoption, but non-network stakeholders are either in the development and implementation phase or taking a wait-and-see approach. At the time of this publication, there were no third-party EMV SRC implementations and only a few merchant adoptions.

The EMV SRC roles and functions include:

- **Digital Payment App (DPA)**:
  Integrates EMV SRC code on websites, mobile browsers, and apps to allow for digital checkout. Requires registration with the EMV SRC System through

---

[20] Cole, S. (2020, Aug. 17). Secure remote commerce and what it means to merchants. *FIS Global*.

[21] A token requestor (TR) is an entity that procures payment tokens from a token service provider (TSP) to use to complete a purchase (e.g., mobile wallet providers, shopping apps, web browsers, card issuers, merchants, acquirers, acquirer processors, and payment gateways). TRs must register and comply with a TSP's proprietary requirements and receive a Token Requestor ID to implement the specified Token API. The TR can then request tokens from the TSP to provision to customer NFC-enabled mobile devices containing secure elements or other storage if using HCE.

an EMV SRC Initiator (SRCi). Examples: marketplace, merchant, hosted checkout page provider.

- **EMV SRC Initiator (SRCi)**:
  Connects EMV SRC components to provide a digital terminal by:
  1) Distributing code to DPAs and registering them with the EMV SRC System
  2) Managing API integration to EMV SRC Systems
  3) Providing checkout data to the EMV SRC System during the transaction, including sending payment card data to the acquirer for authorization.

  Examples: acquirer, gateway, merchant, payment service provider (PSP).

  Distributes code to:
  1) Collect payment card details for system enrollment
  2) Capture consumer authentication data for payment card access via the EMV SRC Systems
  3) Retrieve saved payment card data from EMV SRC Systems
  4) Display the payment card list to the consumer
  5) Connect the consumer to the Digital Card Facilitator (DCF) of the selected payment card
  6) Retrieve the payload from the appropriate EMV SRC System and notify the EMV SRC System of payment authorization.[22]

- **EMV SRC System**:
  Facilitates the digital exchange of information from the digital payment card to the digital terminal to coordinate a payment through a payment card network. Stores the digital payment cards and other data and organizes EMV SRC participant cooperation in the purchase process.
  Examples: card networks, others to be determined.

- **Digital Card Facilitator (DCF)**:
  Delivers the consumer experience to the cardholder and presents the digital payment card for confirmation of the purchase.
  Examples: browser, issuer, third-party wallet provider.

- **Participating Issuer (PI)**:
  Onboards or enrolls consumers into the EMV SRC System and is the source of digital payment card data including cart art and cardholder assurance to establish the authenticity of the consumer identity and PAN.[23]

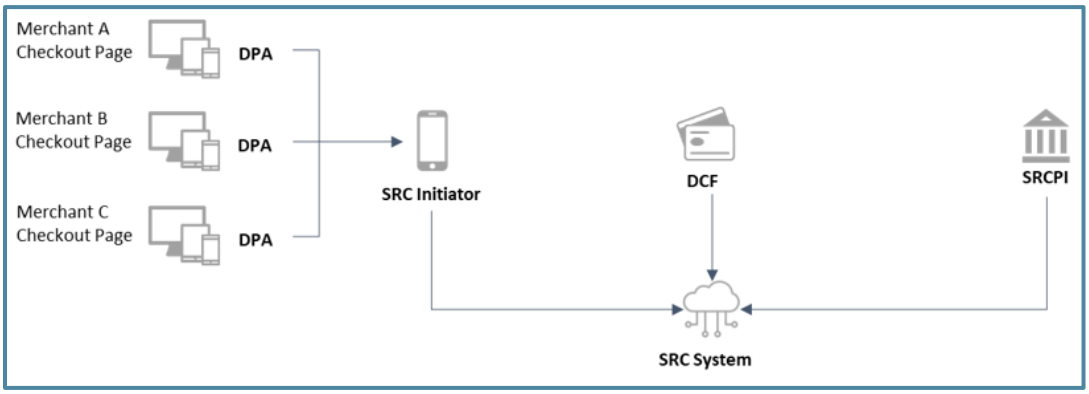
---

[22] Cole, S. (2020, Aug. 17). Secure remote commerce and what it means to merchants. *FIS Global*.

[23] EMV SRC assurance levels address how the card, cardholder, consumer, or the consumer's device is authenticated. Digital certificates are used to sign the applications that initiate SRC transactions, and each app must be registered with each network.

Figure 1 illustrates the EMV SRC process and roles of the parties involved.

Figure 1 – EMV SRC Process and Roles[24]



EMV Secure Remote Commerce Use Cases

EMV SRC can be implemented in different ways, but this whitepaper focuses on first-time customer or guest checkout and returning or known customer.

EMV SRC Use Case 1: First-time Customer – Guest Checkout

To check out on a merchant website a first-time customer selects Click to Pay[25] and sees the first screen image displayed in Figure 2. The customer selects "new user" in the next screen (Image 2). The SRCi requests the customer payment card details,[26] securely directs the payment card data to the appropriate EMV SRC system for enrollment and facilitates the DCF user interface. The customer completes the enrollment and checkout (Image 3). Next, the customer can elect to create a user ID or profile to bind their device to their Click to Pay profile for future use as a returning customer. The customer confirms this information and completes the checkout.

This EMV SRC use case is similar to a typical merchant guest checkout but allows the customer to create a user ID and profile with an email address or other identifier (Image 3). The user ID binds the customer to the payment card and personal information entered.[27] If the customer chooses to have the user ID and profile "remembered" on their device, the EMV SRC System will apply device recognition for future checkouts to streamline the process, as explained in *Use Case 2 – Returning or Known Customer.*

---

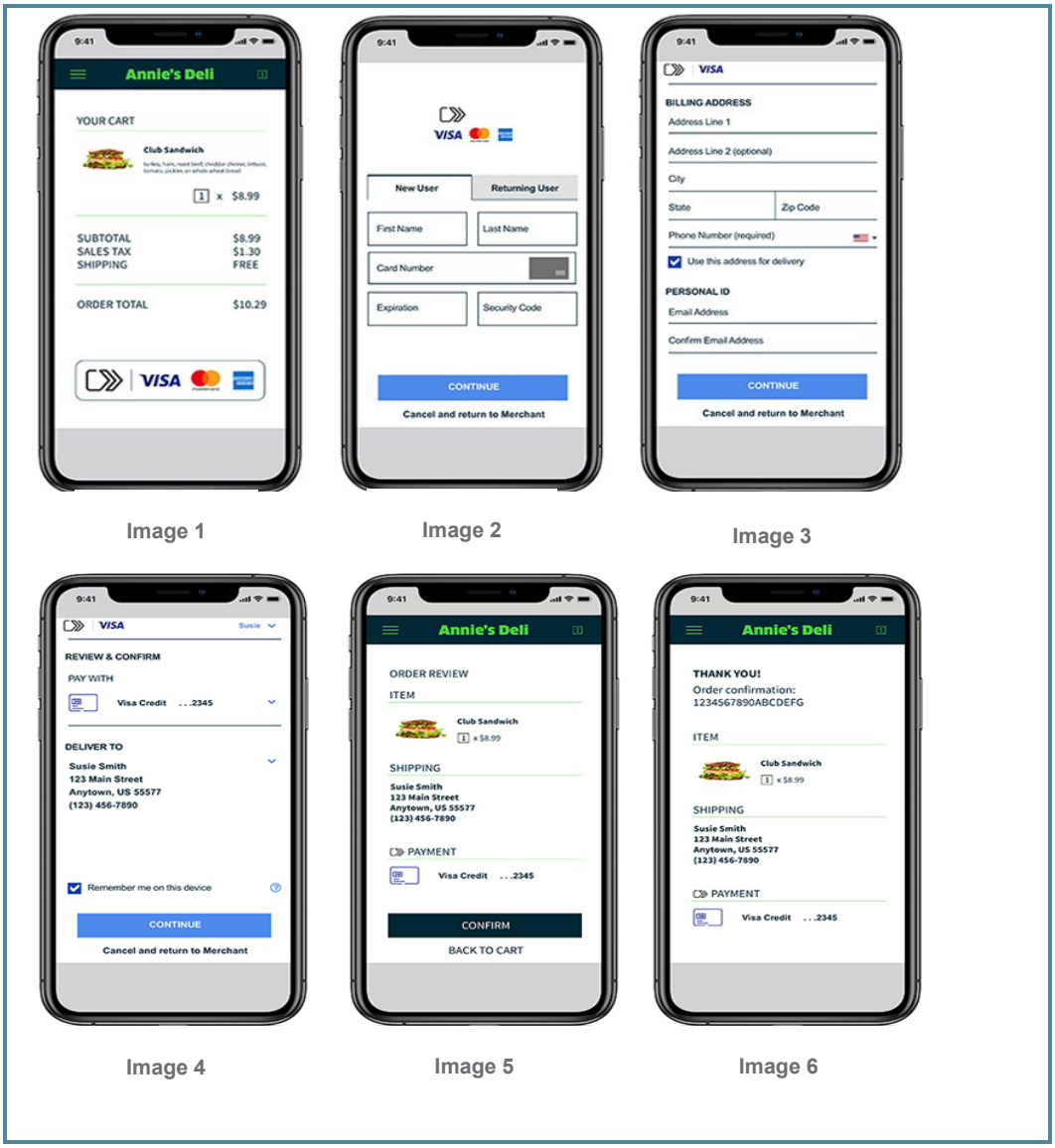
[24] EMVCo. https://www.emvco.com/emv-technologies/src/. Permission to use figure granted by EMVCo on February 24, 2021.

[25] The EMV SRC button displays the Click to Pay icon and payment cards accepted by the merchant.

[26] The payment details provided in this step are used to identify the EMV SRC System (card network) associated with the payment card. The EMV SRC System orchestrates the overall process and facilitates the secure storage of and access to the payment card data. Once the EMV SRC System is identified, the user views a screen to enter the remainder of their billing/shipping information (Image 3).

[27] Cole, S. (2020, Aug. 17). Secure remote commerce and what it means to merchants. *FIS Global*.

Figure 2 – First-time Customer – Guest Checkout[28]



[28] *Ibid*. During the process, the EMV SRC System provides SRCi with a checkout response and requests the payment data for the transaction. The cardholder is returned to the merchant's site to confirm the order. SRCi then initiates the authorization request to the acquirer, which responds with the transaction result. SRCi provides the result to the merchant for display to the customer and notifies the EMV SRC System of the result.

EMV Secure Remote Commerce Use Case 2: Returning or Known Customer

This use case involves a previously enrolled Click to Pay customer with a remembered device and ID/profile. The experience begins with the checkout process (Image 7). When the customer selects Click to Pay, device information is sent to each EMV SRC System to determine recognition of the device. When the device is recognized, the user selects their preferred payment card and completes checkout (Image 8). The order review page displays the relevant personal information the customer previously saved to the EMV SRC System (Image 9). The user then confirms to complete the order (Image 10).

Figure 3 – Returning or Known Customer[29]

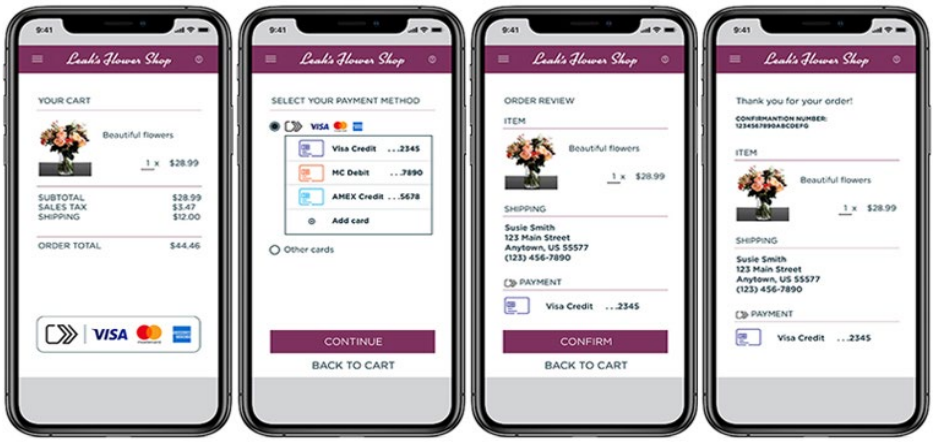


Image 7 **Image 8** **Image 9** **Image 10**

B. EMVCo 3-Domain Secure (EMV 3DS)

3-Domain Secure v1.0 (3DS 1.0) was created 20 years ago to accelerate the growth of e-commerce and reduce fraud by preventing unauthorized credit and debit card use.[30] The three-domain structure represents the merchant/acquirer domain, issuer domain, and interoperability domain. 3DS 1.0 allowed issuers to determine the cardholder authentication method, although the typical method was a PIN or password entered into a pop-up screen[31] during an online purchase. In the U.S., 3DS 1.0 had low adoption because it was browser-based, used static data elements, required

[29] *Ibid*.

[30] Three global card networks have their own implementations of 3DS, Visa *Verified by Visa*, Mastercard *SecureCode*, and American Express *SafeKey*.

[31] Pop-up windows were eliminated in 2005 to allow the cardholder to enter credentials into a browser window.

consumer enrollment, and did not support mobile-initiated payments.[32] Participating merchants experienced high shopping cart abandonment and frustration over their inability to control the consumer experience. However, 3DS 1.0 was widely used in Europe and other countries and became a standard.

In October 2016, EMVCo released a more robust version of 3DS (2.0) to address the shortcomings of the earlier version and the changing global regulatory landscape for e-commerce and CNP transactions. This specification was updated to version 2.2 (EMV 3DS) in December 2018. EMV 3DS provides global interoperability and a consistent consumer experience across mobile app and browser e-commerce channels and connected devices.[33] The protocol permits the issuer to use risk-based authentication (RBA) in the background to prompt step-up authentication (e.g., OTP, biometrics, and out-of-band) for higher risk transactions, significantly reducing consumer friction and replacing static data (e.g., passwords, pre-established question responses, card expiration date).

The protocol adds more than 150 new data elements to help issuers perform a better risk assessment. EMV 3DS sends user data (e.g., shipping address and previous transaction history) and contextual data (e.g., device ID, mobile app, mobile browser) via the payment networks to issuers for input to their risk analysis.[34] The protocol enables four types of data to be shared: transaction and consumer data, authentication data, merchant data, and device data.[35]

Issuers and payment networks must comply with data protection laws and principles to ensure that there is a legal basis for collection of consumer data. Effective RBA (subject to compliance with data protection laws and principles) results in a small percentage (<5 percent) of transactions needing step-up authentication. In addition to mitigating fraud, this reduces issuer operational costs (e.g., number of customer calls about declined transactions to call centers) and increases transaction approvals.

Merchants decide whether to invoke EMV 3DS for higher risk transactions[36] and may share purchase and device data, and other details with the issuer to authenticate the cardholder. Merchants want to maintain low fraud rates while providing a seamless and positive customer experience. They have the option to approve a transaction that 3DS flagged as high-risk because they have more data about the customer. This allows merchants to increase the percentage of legitimate transactions not flagged, limiting step-up authentication to a small percentage of transactions deemed high-risk.

---

[32] Europe realized over 50 percent merchant adoption.

[33] 3DS 2.2 functions separately from v1.0, which will phase out as 3DS 2.2 matures.

[34] Data sent to issuers may also include FIDO and identity data.

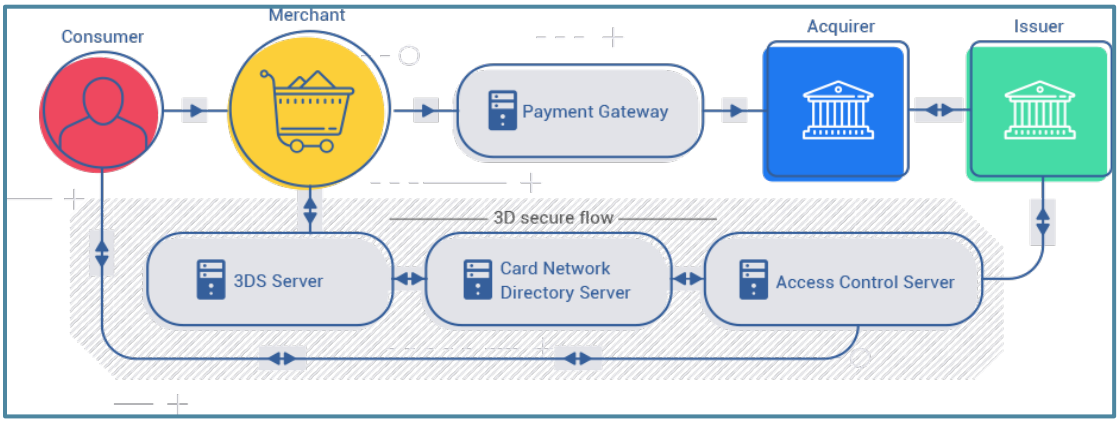
[35] For more information on the types of data included in each group, see U.S. Payments Forum (2020, March). EMV 3-D Secure.

[36] A transaction may be flagged as high-risk based on a company's risk-decisioning model (e.g., when a customer's mobile device used to make a purchase does not match the previous mobile device used by that customer).

Based on the customer risk profile, the issuer can use RBA to authenticate the cardholder passively or invoke step-up authentication. Issuers maintain control of the authentication flow because they are liable for all EMV 3DS-initiated transactions that they approve. This liability will also shift back to issuers who have not upgraded to EMV 3DS in 2021 (exact date TBD). Therefore, the issuer may require step-up authentication for unusual or high-value purchases or to meet regulatory requirements.

Figure 4 provides a basic overview of the EMV 3DS flow.

Figure 4 – EMV 3DS Flow[37]



Some U.S. companies that do business in the EU are developing strategies to deploy EMV 3DS in response to the EU's Payment Services Directive 2 (PSD2) Strong Customer Authentication (SCA) requirement, first implemented in September 2015.[38] The objective was to regulate payment services and providers throughout the EU and European Economic Area. The EU updated PSD2 in September 2019 to define the SCA standards for online payments. EU FIs must comply with PSD2-SCA by the end of 2020, and all other stakeholders by early 2021. Most are implementing EMV 3DS to satisfy the requirement. Large technology companies, such as Amazon, Apple, Google, and PayPal, are already SCA-compliant.

---

[37] 3DSecure2 (n.d.). https://3dsecure2.com/. Permission to use figure granted by EMVCo on February 24, 2021.

[38] PSD2 is a data and technology-driven directive to increase competition, innovation, and transparency across the European payments market, while also enhancing the security of Internet payments and account access. PSD2 SCA is a process to confirm the user's identity through a minimum of two different and independent authentication factors. This applies to sensitive banking operations and electronic payment transactions. Using the card number and an SMS OTP is no longer compliant with the mandate. The industry is moving towards app-based authentication, and EMV 3DS is required by all participants. SCA is designed to protect the confidentiality of the authentication data and requires use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses), and inherence (something the user is) that are independent, so the breach of one does not compromise the reliability of the others.

PSD2 promotes new payment services and enhances consumer protection and security. SCA stipulates that two-factor authentication (2FA) is required for all electronic payment transactions, with some exemptions. U.S. merchants with sales to European consumers need to upgrade their authentication capabilities to allow for 2FA, or transactions will be declined. EMV 3DS is widely adopted across Europe, and provides improvements that consider SCA regulatory requirements, the need to support digital wallets and other payment modes, and declining conversion rates. This is noteworthy because SCA is not mandated in the U.S.

The key benefit of any remote payment technology is to drive improved transaction authorization rates, reduce fraud, and increase merchant sales. The specific benefits of EMV 3DS include: 1) improved consumer experience through less friction; 2) universal device support, such as native apps, digital wallets, and non-payment authentication; and 3) opportunity for greater data sharing, with 10 times more data that can be shared between merchants and issuers to enhance RBA. For a comparison of 3DS 1.0 data to the enhanced data elements for EMV 3DS, see Appendix A.

C. FIDO Alliance and Authentication Platforms

FIDO, founded in 2012, is an open industry association that develops and promotes specifications and certification programs to help move the world beyond passwords with simpler, stronger authentication. The FIDO Alliance's goal is to shape the authentication landscape by developing standards that enable authentication tools that are more secure than passwords, usernames and SMS OTPs, as well as easier for consumers to use and for service providers to deploy and manage. FIDO specifications enable users to leverage common devices, such as built-in biometrics or external security keys, to authenticate to online services in both mobile and desktop environments.

FIDO technology shifts organizations away from reliance on server-based static data elements such as passwords to on-device public key cryptography, increasing the security of user authentication while making it easier for the user. FIDO Alliance is collaborating with EMVCo and W3C to assess the impact of these protocols for future authentication management (e.g., transaction data flows using EMV 3DS and Consumer Device Cardholder Verification Methods (CDCVM))[39] and authenticator certification programs. The need to enhance security while providing a more optimal customer experience is driving this shift.

FIDO Alliance defines technical standards for fast, strong, on-device "authenticators" built into internet-connected devices. In 2014, FIDO released two sets

[39] Consumer Device Cardholder Verification Method (CDCVM) is a consumer verification method (CVM) supported by the card networks when assessing transaction originating from mobile devices. Verification is used to evaluate whether the person presenting the payment instrument is the legitimate owner of the instrument.

of specifications, Universal Authentication Framework (UAF)[40] and 2nd Factor Authentication (U2F).[41] These specifications support a wide range of authentication modalities, including biometrics and PINs. The FIDO Alliance's latest strong authentication specification, FIDO2, expands FIDO authentication across browsers and related web platform infrastructure. FIDO2 is comprised of the W3C WebAuthn specification and FIDO CTAP,[42] which expands authenticator interoperability with client platforms. WebAuthn defines an API that enables web apps to create and use strong, attested, scoped, public key-based credentials to strongly authenticate users.

FIDO2 can be used as a second factor, like U2F, or for passwordless authentication with FIDO-defined private keys stored on the device. FIDO credentials are applied when an application or web service uses FIDO2 for account authentication.[43] The certification testing for FIDO authenticators and servers enables a secure and consistent user experience across all the apps a consumer may use.[44, 45]

Companies that have deployed FIDO-compliant mobile app solutions in the U.S. include Cigna, eBay, Intuit, and T-Mobile. Relying parties[46] can add browser-based FIDO SCA solutions (as well as the previous mobile app-based solutions) on any device that supports a Chrome, Edge, Firefox, or Safari browser.[47] FIDO2 enables the new browser-based FIDO capabilities.

D. W3C – WebAuthn and Payment Request/Payment Handler APIs

The W3C is an international community with members that represent large technology companies, mobile operators, large FIs, merchants, and other organizations that collaborate to develop web standards and guidelines for a rich set of web capabilities that can work on any device.[48] Key goals of W3C's payments standardization efforts include streamlining checkout and reducing fraud. The standards process promotes

---

[40] A user registers their device to an online service with a local authentication mechanism such as a fingerprint or facial recognition, a mobile phone's camera functionality, microphone, or PIN entry. Once registered, the user repeats this action whenever the service requires authentication. The online service decides which mechanisms to present to the user. The result eliminates the need for user passwords.

[41] For more information on U2F, see https://fidoalliance.org/specifications/. FIDO is now an official International Telecommunication Union (ITU) and International Standards Organization (ISO) standard.

[42] For more information on CTAP, see https://fidoalliance.org/specifications/.

[43] PayPal and Samsung were first to publicly deploy FIDO authentication in 2014.

[44] When a device establishes a preferred locking method such as a fingerprint, it can make that authenticator available to app developers through a common API resulting in a common authentication experience across all apps, including payment apps on that device. FIDO is an open standard that device manufacturers add support for in these APIs.

[45] FIDO is also working with W3C to standardize FIDO authentication in APIs for web app developers.

[46] A Relying Party is a server providing access to a secure software app (e.g., software running on mobile devices), which can be used to grant user access to software apps, but also for secure building access, without the user entering their credentials each time.

[47] With the support of Google, Microsoft, and Mozilla,

[48] For a full list of members, see https://www.w3.org/Consortium/Member/List.

consensus, fairness, public accountability, and quality. W3C publishes "Recommendations," which are considered "Web Standards." This section reviews the *WebAuthn* and *Payment Request and Payment Handler* APIs.[49]

WebAuthn

The WebAuthn specification is intended to provide strong authentication and reduce login friction for users. W3C, in coordination with the FIDO Alliance, published WebAuthn Level 1 in March 2019 and a working draft of Level 2 in November 2020. Its goal is to standardize an interface for authenticating users to web-based apps and services using public-key cryptography.[50] The API allows servers to integrate with strong authenticators (e.g., fingerprint or facial recognition) built into devices. The private key is stored securely on the user's device, while the server receives a public key and randomly generated credential ID for storage and uses that public key to prove the user's identity.[51] WebAuthn is also resilient to active man-in-the-middle-attacks. Moreover, a roaming hardware authenticator is resistant to malware since the private key material is at no time accessible to software running on the host machine.

Payment Request and Payment Handler APIs

In 2018, the W3C Web Payments Working Group introduced the Payment Request and Payment Handler API to help reduce shopping cart abandonment and speed up checkouts. The final recommendation or standard is anticipated in early 2021.

The *Payment Request* API streamlines checkout by:

1) Re-using stored data
2) Offering a consistent and faster Web checkout experience
3) Reducing merchant integration costs
4) Using one standard integration API versus multiple proprietary ones.

The *Payment Handler* API:

1) Encourages innovation through Web-based Payment Handlers ("wallets")
2) Provides a fast, harmonized, browser-based user experience
3) Provides a modal window for Payment Handlers to preserve the merchant context
4) Anticipates higher successful transaction completion rates and better security.

The Payment Request API standard allows merchants (i.e., websites selling physical or digital goods) to utilize one or more payment methods with minimal integration effort. Web browsers facilitate the payment flow between the merchant and user.[52] The API improves the consumer experience as an enhancement to web autofill, particularly for mobile users, by reducing the need for information entry. Since

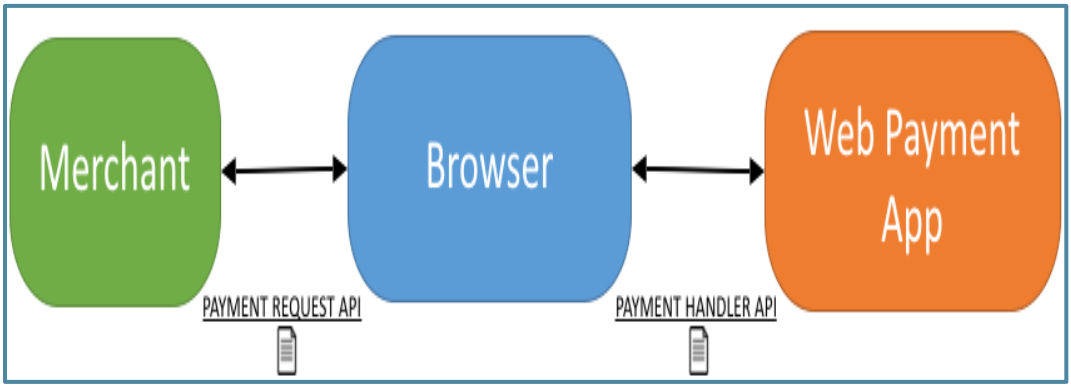
---

[49] These specifications or recommendations can be found at www.w3.org.
[50] The authenticator performs underlying cryptographic operations.
[51] The public key is not secret because it is effectively useless without the corresponding private key.
[52] Per the Payment Request API specification, the user agent (e.g., browser) acts as an intermediary between three parties in a transaction: payee (merchant online store, or other party requesting payment), payor, who authenticates the payment, and payment method (e.g., card payment).

2018, the Payment Request API has been implemented in many desktop and mobile browsers. It can be used with Apple Pay (with Safari), Google Pay, PayPal, and Samsung Pay. Chrome, Edge, Opera, and Samsung also allow other payment apps to be used with Payment Request API, either native (on Android) or Web-based (through the Payment Handler API).

Similar to EMV SRC, Payment Request helps to streamline guest checkouts and minimize friction for returning shoppers. The API works with multiple payment methods in addition to payment cards. The shopper selects a saved payment method and confirms the purchase in the payment user interface provided by the browser. Subsequently, the credential should appear when the web browser is on an e-commerce merchant site that accepts that credential. Figure 5 shows how the Payment Request API interacts with the other participants in the payments process.

Figure 5 – Payments Request API Interaction[53]

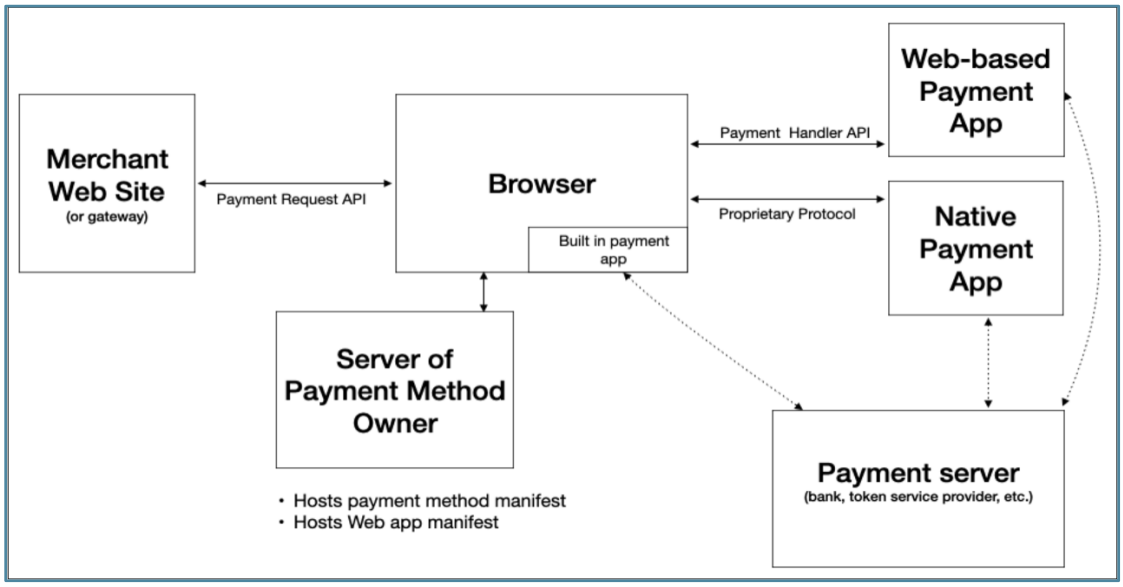


The Payment Handler[54] API offers front-end integration and ease of user experience for making payments on the web. Payment handlers may be implemented as Web pages, native mobile apps, or built into the browser. When a user selects a "buy" button, it triggers the API, which displays multiple Payment Handlers for the consumer to choose from. The nature of the interaction and the authentication process depends on the Payment Handler.

[53] Permission granted from Ian Jacobs, W3C on February 9, 2021. See www.w3c.org.
[54] A Payment handler is user software to make a payment. Payment Handler Security, Web Payment Working Group, W3.org.

Figure 6 illustrates how the respective elements of the flow are connected.

Figure 6 – Connecting the Elements[55]



Apple Pay and the Payment Request API

Apple Pay's web payment solution leverages the W3C Payment Request API. Apple Pay on the web was first released in Safari on macOS Sierra and iOS 10 in 2016. Apple Pay brought ease-of-use, security, and privacy to online transactions and received widespread adoption by merchants. However, merchants still need to support multiple payment methods, which adds complexity. When the W3C Web Payment Working Group produced a first working draft of Payment Request API, Apple added support in Safari 11.1 on macOS, and Safari on iOS 11.3, in April 2018. Payment Request aims to reduce merchants' integration complexity by supporting various payment methods across multiple browsers using the same standard API.

EMV SRC and the W3C Payment Request API

The Web Payments Group goals for EMV SRC include:

1) Ensuring availability of Payment Handlers
2) Identity management
3) User experience.

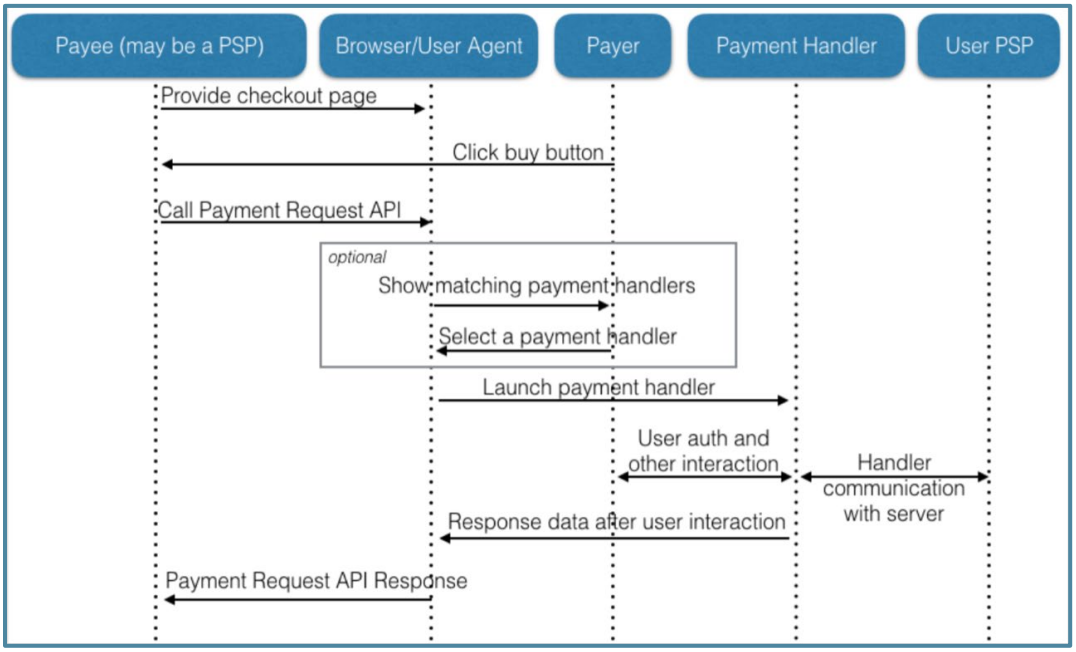
In 2018, EMVCo and W3C collaborated to create synergies between their respective ecosystem by considering the Payment Request API as one possible solution for implementing EMV SRC. Both protocols want to solve the same industry challenges

[55] Permission granted from Ian Jacobs, W3C on February 9, 2021. See www.w3c.org.

related to ecosystem complexity and friction in the checkout process. While W3C addresses a wide range of payment methods with minimal integration for web transactions, EMVCo is broader and focuses across different devices and environments, but only for card-based payments.

The W3C Payment Request API defines a new browser capability that simplifies and increases the speed for merchants to request payment and for users to checkout using information stored in the browser (e.g., addresses, payment credentials). The merchant uses an API to present its supported payment methods to the user (e.g., buy button). If only one payment method app matches what the merchant accepts, the browser automatically launches it. If multiple payment method apps match, the browser prompts the user to select one to complete the transaction. The browser returns data from the payment method app to the merchant (or their PSP, the party that calls the API). The API defines how these payment apps register their payment methods with the browser, how the browser launches the payment app, and how the payment app returns data after completion of user interaction.[56] This API and payment apps operate with a variety of payment methods. Figure 7 illustrates an example of an API-enabled user journey, with optional selection of payment method app.

Figure 7 – W3C API User Journey with Optional Payment App Selection[57]



[56] W3C, FIDO Alliance, and EMVCo (2020, Nov. 5). *How EMVCo, FIDO, and W3C technologies relate.* https://www.w3.org/TR/2020/NOTE-htr-20201105/. How a payment app stores information, authenticates the user, and communicates with payment services (e.g., token service providers, issuers, etc.) lies outside the scope of the API.

[57] Permission granted from Ian Jacobs, W3C on February 9, 2021. See www.w3c.org.

Web Payment APIs can be interoperable with EMV SRC by using the browser to access the functionality of the EMV SRC System roles. For example, a Payment Handler can serve as a Digital Card Facilitator (DCF) under EMV SRC, which would require access to consumer payment card data stored in the EMV SRC System. This interoperability can reduce repetitive manual user data entry and decrease cart abandonment. EMV SRC and the W3C Payment Request API[58] could be integrated for first-time user enrollment. Appendix A shows a potential integration scenario for an EMV SRC and W3C Payment Request for a first-time user enrollment.

When an EMV SRC transaction begins, the SRCi performs the assurance and validation steps to bind the cardholder to their device. The SRCi also collects information to send a customer profile request to the EMV SRC System. Hypothetically, the SRCi could leverage W3C WebAuthn to perform this function.

The EMV SRC System would return a customer profile response presented by a DCF (i.e., Candidate List) to allow the customer to select the desired payment card.[59] The SRCi would then send a Checkout Request with information about the selected payment card (e.g., shipping and billing addresses, risk data).

After the consumer selected their preferred payment card, the SRCi would send a payload request, and the EMV SRC System would respond with a payload that includes dynamic data. The payload response allows the SRCi (and ultimately the merchant) to create a traditional authorization request. Once the authorization request was sent (via merchant gateway/PSP/acquirer) and an authorization response received (i.e., authorized or declined), the SRCi could send a confirmation request to the EMV SRC System to signal the end of the transaction and receive a confirmation response in return.[60]

An SRCi is required to register with the respective EMV SRC Systems and enroll each DPA that it supports. A W3C Payment Handler would need to develop a scheme to register each website that it supported. Some *handler-like* implementations (e.g., Apple Pay and Google Pay) already require website registration. Therefore, other Payment Handlers would need to implement similar processes to work with SRC.

---

[58] The Payment Request API allows a merchant to request payment from a buyer, with the browser serving as the interface to capture a person's necessary payment details. W3C Website Payment Standards for Secure Web Payments | American Express

[59] While the DCF may not interact with the cardholder, the DCF may offer a user interface within the SRC specs. The SRCi must present all the EMV SRC enrolled payment cards in a Candidate List associated with the cardholder. The Candidate List displays payment cards based on the most recent card used. However, the Payment Handler API can allow a user to control this ordering.

[60] The existing Payment Request API may not be able to satisfy the requirement to send a confirmation request from the SRCi to the EMV SRC System The current Payment Request specification allows for a "complete" method to be called, but its result can currently only be a "success," "fail," or "unknown." Sending confirmation requests may require an extension to carry the additional information required, however they are optional in the current SRC spec.

Payment Request adoption remains a challenge, but the Web Payments Group is considering enhancements to the API. One card network is working with W3C to develop an EMV SRC System Payment Handler.

EMVCO, FIDO Alliance, and W3C Collaboration

Identifying opportunities for alignment is an ongoing process. In April 2019, EMVCo, FIDO Alliance, and W3C formed the Web Payment Security Interest Group to collaborate on a vision for web payment security and interoperability and to address gaps and overlaps between EMV 3DS, EMV SRC, W3C Payment API specifications, and WebAuthn and FIDO specifications. For example, they have worked together to provide consumer access to digital payment cards and facilitate a secure, low friction checkout experience.

W3C also created a separate business group for merchant participation. Based on interviews with some industry stakeholders, general W3C participation is difficult unless the participant has extensive technical and engineering expertise, including cryptography and programming skills. However, many stakeholders remain interested in participating to stay abreast of developments. Merchants, in particular, are interested in efforts to develop open industry standards. Many stakeholders agree that the ecosystem would benefit from more open browsers than solutions that are operating system specific.

The organizations also meet to share experiences and expertise in security and privacy to help address industry confusion They provide information about the technologies as well; for example how they may interoperate, and how to ensure that one solution does not create security gaps for another solution.[61]

W3C leverages its expertise to focus on enhancing browsers to create a more intuitive experience for making payments. FIDO Alliance focuses on authentication, not the payment itself. FIDO Alliance seeks to offer strong cryptographic proofs that the person is the same person as the last visit (with fewest clicks and least friction possible). Finally, EMVCo focuses on services specific to card payments.[62]

III. Stakeholder Perspectives

One of the key objectives of this whitepaper is to present industry perspectives on how the specifications can improve the remote consumer experience, while also improving security, and share their views on implementation and adoption progress. The information covered in this section is based on approximately 15 interviews with industry stakeholders who represent card networks, FIs, acquirers, gateways,

[61] In November 2020, the FIDO Alliance held an Authenticate Conference for stakeholders to collaborate. See https://virtual2020.authenticatecon.com/s/landing-page5/home.

[62] Appendix C provides a list of publications released by these groups to demonstrate their collaboration efforts on the protocols.

processors, merchants, digital wallet providers, technology providers, and industry groups.

A. EMVCo Secure Remote Commerce (EMV SRC)

While officially launched in December 2019, EMV SRC is still in the early stages of adoption among all payment stakeholders.[63] There are two phases to adoption. The first phase requires stakeholders supporting previous versions of network digital wallets to replace those wallets and migrate to the consumer-facing version and new brand name, Click to Pay. The second implementation phase is a full integration that requires more work by the card issuers and card networks to enroll and provision consumers, and to increase participation of stakeholders to onboard merchants. Merchants must also decide whether to include EMV 3DS and/or EMV tokenization, which are optional, but can strengthen authentication in the checkout process.

Card Network Perspectives on EMV SRC Click to Pay

The card networks developed the EMV SRC spec to address the fragmented merchant guest checkout by delivering a common experience. EMV SRC brings the in-store level of payment consistency (via chip card) to online payments, particularly when the consumer enters payment credentials for the first-time on the website. EMV SRC's key benefits are ease of checkout, improved user experience, and better security through the elimination of usernames and passwords.

Re-branding the card network digital wallets to Click to Pay on merchant websites has been completed for approximately 90 percent of U.S. merchants.[64] The networks spent a considerable amount of time helping merchants minimize the impact of this transition. Now they are focused on enabling more merchants and building adoption by partnering with acquirers, gateways, and processors to expand EMV SRC roles and support multiple clients. Collaborating with industry stakeholders will also drive overall innovation.

One card network reported that adoption is still in the early stages and only a fraction of its transactions occurs through Click to Pay. However, COVID-19 has increased the number of consumers shopping online for groceries and other household items to avoid shopping in-person. Network data reflect more first-time online shoppers and more shopping in new categories. Promoting Click to Pay security benefits to first-time online shoppers can lead to repeat online customers, particularly if their concerns about sharing credentials online are addressed.

EMV SRC benefits merchants transitioning to the digital environment, merchants with higher proportions of guest checkouts, and those using card-on-file (CoF) network

---

[63] Early merchant adopters include: BassPro, Cinemark, Crate & Barrel, Expedia, Fresh Direct, Joann Fabric and Crafts, JoS. A. Bank, Lowe's, Marriott, Movember, Netflix, Papa John's, Rakuten, Saks Fifth Avenue, SHOP.com, Staples, and Tickets.com.

[64] This migration pertains to merchants that already supported the card networks' digital wallets, so implementation only involved re-branding to Click to Pay.

tokenization. If merchants typically collect anonymous payment card information from a first-time customer via form-fill they will also benefit from EMV SRC.

Gateways and processors provide education primarily to smaller digital merchants on behalf of the card networks. Smaller merchants tend to have one-time or infrequent customers (i.e., guests), creating an opportunity for EMV SRC to remove friction in the transaction. Beyond basic implementations, gateways and processors have the opportunity to create EMV SRC experiences that are unique to the merchant (e.g., checkout page design) by serving as an SRCi.

The card networks believe that EMV SRC can provide customers with familiarity and habituation by recognizing a common icon, much like contactless transactions that display a wave-like symbol. This experience is consistent regardless of the type of device used or type of merchant. EMV SRC creates a foundation for consumer confidence that can be leveraged as payments migrate to new channels, e.g., payments from a car, watch, or appliance, etc., in the future.

EMV SRC enables a secure remote experience with less friction. The result is lower fraud, less abandonment, and increased approval rates. The card networks are seeking broader industry participation to drive adoption. The EMV SRC spec was designed to be forward-looking and its value to merchants will depend on how it is delivered by the SRCi, gateway, and digital card facilitator (DCF) (e.g., wallet provider or browser).

The card networks explained that EMVCo defines the EMV SRC integration process, and the SRCi uses standard interfaces to connect with each card network. This enables a stakeholder to build the interface once and then apply it across all networks or endpoints. The card networks concur that the EMV SRC spec itself is sound, and also agree that improvements can be made to the merchant checkout experience to reduce friction, which will eventually be managed by the DCFs. They contend that without EMV SRC adoption, merchants will encounter increased shopping cart abandonment and more CNP false declines.

Merchant Perspectives on EMV SRC/Click to Pay

According to an American Express 2019 Digital Payments Survey, which reviewed the current status of U.S. online and in-store payments, 80 percent of merchants said they would benefit from technology that reduces the need to store customer payment data, and 79 percent agreed that their online checkout experiences need to be simplified for customers.[65] Similar to digital wallet solutions, the EMV SRC spec addresses these needs and describes how merchants can facilitate payment authorization for remote commerce transactions using Click to Pay to eliminate storage of customer payment credentials and streamline the checkout experience. EMV SRC does not redesign the merchant checkout experience but does make it more efficient and secure.

[65] American Express (2019). *2019 Digital Payments Survey*.

Merchants have two options for implementation. Merchants that previously supported the card network digital checkout wallets can convert them to Click to Pay on their checkout page. Alternatively, merchants can opt for full EMV SRC integration where the merchant becomes an SRCi or works with an SRCi (e.g., acquirer, gateway, processor) to connect to each EMV SRC System. While full integration requires more work, the merchant has more control over the customer experience as an SRCi. Merchants that support alternative payment methods will need to weigh the benefits of EMV SRC against the ease of use of other methods, customer reactions, and potential disruption.

For merchants that support guest checkout, EMV SRC can provide a secure, streamlined method for customers to access their payment card information, eliminate redundant entry of shipping and billing addresses, and potentially minimize storage of data that requires Payment Card Industry Security Standards Council (PCI-SSC) compliance. Merchants agree that EMV SRC is best suited for guest checkout and that they will realize more benefits from an improved customer experience. However, some merchants are considering elimination of guest checkout because they experience more fraud.[66] EMV SRC may offer those merchants a way to keep guest checkout and provide a better customer experience.

The interviewees concur that small to mid-sized (SME) merchants with a high ratio of guest checkout transactions are best suited to adopt Click to Pay. These merchants need a secure checkout process that results in higher conversion rates and less fraud. SME merchants also benefit by removing maintenance of customer CoF databases. Furthermore, implementing EMV SRC may allow smaller merchants to leverage other card network features in a seamless manner (e.g., EMV tokenization, EMV 3DS, CoF, etc.).

EMV SRC is a good option for SME merchants if their service providers or acquirers offer it. However, the larger merchants with major investments in payment flow optimization may hesitate to adopt EMV SRC until EMV 3DS adoption increases, which would shift liability to the issuers.

A large online retailer noted several key issues that need resolution before deciding whether to implement EMV SRC:

- Inability to enroll a co-branded merchant payment card in EMV SRC (merchants also want their cards available through EMV SRC)
- Order of payment cards presented to the customer in the Candidate List at checkout (i.e., merchants want their payment card to be top of wallet)
- Compliant debit routing options[67]
- Customer experience impact.

[66] Interviewee communication, October 26, 2020.

[67] Debit routing is a concern because it is unclear how it will work with EMV SRC.

Currently, Click to Pay displays the last payment card used by the customer in the Candidate List. If a customer previously shopped with Merchant A, but then made a Click to Pay purchase with Merchant B, the Candidate List would present Merchant A's payment card at the top of the list. While the customer can scroll through the list and select their preferred payment card, merchants worry that customers may just select the last payment card used. This is particularly concerning to merchants that sell high-value merchandise where customers shop less frequently, so their payment card might not be at the top of the list. The next iteration of EMV SRC is expected to allow merchants to create a feature that enables the customer to select their co-branded card as top of wallet.

Merchants reported some unexpected customer experiences, possibly attributed to the newness of Click to Pay, which is why some would like to see more results before they implement the function, as well as education for consumers about what Click to Pay is and how to use it. Merchants view development of customer education and awareness as a joint effort between merchants and card networks.

Click to Pay offers merchants an integrated solution across card networks, eliminating the need to manage different rules and integration requirements for each card network's preferred checkout mechanism. To address growing e-commerce fraud, Click to Pay also includes strong security and fraud prevention tools. For example, EMV tokenization and dynamic data protect a consumer's card credentials by removing them from the payment process. In summary, EMV SRC can help the merchants by reducing purchase time, customer friction and potential cart abandonment, leading to more satisfied customers and improved profits.[68]

Issuer Perspectives on EMV SRC/Click to Pay

Most large issuers support Phase 1 of EMV SRC (i.e., initial conversion of digital wallet cardholders to Click to Pay). Only a few have moved to the onboarding and provisioning phase. Issuers prefer to onboard customers via their online or mobile banking platforms, instead of through the merchant site or other channel, as this gives them greater control over their customer's experience. They also see EMV SRC as an opportunity to replace the "NASCAR" model,[69] which displays many checkout buttons on a merchant website, each offering a custom checkout experience. Issuers emphasize that having only one button helps to mitigate online transaction fraud that alternative payment models may be exposed to each time they add new users and payment credentials.

Generally, issuers want more adherence to card network protocols to protect their customers and the overall ecosystem. For example, data collected through EMV SRC and EMV 3DS support issuer efforts to automate the dispute process. EMV SRC also

---

[68] Another benefit of EMV SRC is the inclusion of dynamic data and customer/cardholder-related data in the payload response The specific content of the payload response is determined by service request indicators and may include any of the following data elements: PAN, BIN, product type, shipping address, e-mail address.

[69] NASCAR model shows racecars covered with multiple sponsor logos.

offers a centralized approach that provides greater visibility into potential payment risk or fraud events, payment authentication, and enhanced authorization.[70]

Issuers understand that EMV SRC is a good alternative to existing guest checkout processes and most suitable for SME merchants. They believe that the fastest way to adoption is for those merchants to work with their acquirers and gateways to host the checkout pages and add the Click to Pay button. Consumers will benefit from less manual entry data needed to complete a transaction, which will decrease shopping cart abandonment, reduce input errors, and increase overall transaction security.

EMV SRC binds the customer's credentials to their device, which are recognized each time they use Click to Pay to transact. If EMV 3DS is invoked and returns a low-risk response from the access control server (ACS),[71] then the issuer may not have to authenticate the user. While EMV SRC does not require the merchant to adopt EMV tokenization or EMV 3DS, issuers believe that many stakeholders (issuers and merchants) are including tokenization with their EMV SRC implementations.

Like merchants, issuers also want their payment cards top of wallet in the EMV SRC Candidate List. They are less concerned about converting cardholders from card network digital wallets to Click to Pay and prefer to work simultaneously with multiple network capabilities.

Smaller issuers may not have their own authentication/fraud systems, nor are they directly represented at EMVCo (although processors and issuer acquirers may represent their interests). The issuers may only have rudimentary knowledge of these protocols, and not fully understand their benefits. They rely on processors and acquirers to help them enable EMV SRC and EMV 3DS and provide education.

Most issuers agree that it is too soon to predict the timing of broad EMV SRC adoption, although demonstrated success achieved by early adopter merchants and growing issuer support will help.

Acquirer and Processor Perspectives on EMV SRC/Click to Pay

Many third-party acquirers and processors are working with all card networks to implement EMV SRC. Similar to other stakeholders, their first phase of implementation involves migrating card network digital wallets to the re-branded Click to Pay. Third-party acquirers and processors that support payment tokenization or network digital wallets do not need to make any changes to enable Click to Pay, other than communicating the new branding to customers.

The implementation process is more complex for third-party processors because the card networks are at different stages of maturity. Visa and Mastercard led the initial drive for EMV SRC implementation, while American Express and Discover only

---

[70] EMVCo, https://www.emvco.com/emv-technologies/src/.

[71] Currently, there are very few ACSs in the U.S., which include card networks (e.g., Cardinal Commerce owned by Visa), RSA Security (owned by EMC), CA Arcot, and Oracle. Some U.S. companies may serve as ACSs in other countries that may shift these services to the U.S. in the future.

recently launched Click to Pay. Processors want the card networks to move beyond Phase 1 and expand the market user base. However, the card networks' plans are still in development, with only a few live merchant EMV SRC implementations, impeding customer adoption.

Although the card networks still support all EMV SRC roles (e.g., SRCi, EMV SRC System, DCF, DPA, etc.), acquirers and processors anticipate performing the SRCi role in the future. The card networks want wider industry collaboration and participation, but there is a lag between releasing the specification and developing APIs for third-party providers. The EMV SRC implementation phase for an acquirer or processor can range from six to 12 months, which includes developing different approaches for each network and ensuring consistent customer experiences.

Many issuers have not yet augmented their risk models to support EMV SRC transaction processing and enable additional data to achieve fraud benefits from EMV SRC and EMV 3DS.[72] Without the new data a merchant cannot distinguish the e-commerce transaction as Click to Pay, and take advantage of the new security features. Without Click to Pay data, the merchant must review the transaction based on previous risk decisioning rules, which offer no lift in authorization rates or additional reductions in fraud. However, stakeholders are hopeful that this barrier to adoption will be addressed in the future

Processors see a lift in authorizations from issuers that have adapted their risk models to accommodate the new data. However, there is a lack of consistency across the ecosystem. Acquirers and processors believe they could make a better argument to merchants to support these protocols if they could document specific benefits in terms of increased authorization rates and reduced fraud. However, merchants are reluctant to share more data with third-party providers because they want to know the data will not be used to competitively disadvantage the merchant. This is a difficult challenge to overcome with merchant customers.

According to acquirers and processors, EMV SRC consumer enrollment remains a challenge for both merchants and issuers. Currently, the primary method for consumer enrollment is to select Click to Pay through the merchant website. Merchants do not like this option because it makes them responsible for consumer enrollment in a card product, versus a merchant payment product. The consumer must also create an EMV SRC User ID during the enrollment and they may not understand that they are only using the merchant site as a conduit to the card issuer. The consumer may think their personal information is being shared with the merchant, which is not the intent of most guest checkout customers. New EMV SRC requirements may address this enrollment experience and offer enrollment through issuers, which is considered essential for future adoption.

---

[72] Completing Phase 1 (Click to Pay conversion) does not guarantee that changes are propagated to the issuer's risk models.

Digital Wallet Perspectives on EMV SRC/Click to Pay

The expanding growth of the e-commerce market, along with consumer desire for payment choice, creates the opportunity for multiple digital wallet options. In addition to the EMV SRC spec, existing PSP solutions (e.g., Apple Pay, Google Pay, and PayPal) have realized strong consumer and merchant adoption. While digital wallet payment options have created innovation in the market, usage is still low compared to overall payment card entry/guest checkout volumes.

Generally, digital wallet providers believe that large merchants and platforms serving smaller merchants will decide, based on conversion, which "buy" buttons to accept on their sites that will optimize consumer choice and allow co-branded and private label payment card credentials as top of wallet. They do not see a need to bring the in-store level of payment consistency (via chip card) to online payments, noting that digital wallets offer a first-time checkout experience that does not require the consumer to reveal payment credentials directly to merchants. Some merchants may need to compare the benefits of existing digital wallet solutions, which provide similar attributes, including ease of checkout, user experience, security and elimination of username and passwords, to those offered by EMV SRC.

Digital wallets and EMV SRC use different approaches to provide similar benefits to consumers. Digital wallet providers observe that the primary benefits offered by EMV SRC drive value by replacing each instance of a key-entered payment card with an alternative experience that is frictionless and more secure are the same benefits offered by digital wallets, which also leverage payment tokenization. They encourage the card networks to move quickly to a fully tokenized solution for all merchants migrating to EMV SRC.

Digital wallet providers work with industry stakeholders to serve smaller merchants by removing user friction and building habituation. The wallets provide a consistent consumer experience for in-app and website checkout. They are characterized by lower fraud, less abandonment, and increased approval rates. Some of the digital wallet providers (e.g., Amazon Pay, PayPal, Shop Pay, etc.) also provide post-transaction services, such as order tracking or buyer protection, that minimize customer service calls and further decrease friction. Overall, digital wallet providers do not agree that shopping cart abandonment or CNP false declines, for example, will increase without broad EMV SRC adoption.

EMV SRC/Click to Pay Summary

EMV SRC provides a virtual terminal that models the POS experience in the digital payments environment and delivers a digital payment card to the issuer. The underlying transition occurs from a key-entered cardholder credential-on-file to an issuer-authenticated digital form factor.

Improving the guest checkout experience particularly benefits smaller merchants that do not manage their own e-commerce process. The added convenience and

security of not entering payment credentials on a merchant site should encourage more guest shoppers to complete online purchases.

The anticipated EMV SRC end-state includes combining EMV tokenization and EMV 3DS and creating a common specification. This requires infrastructure that can accommodate all three protocols and is easy to implement across the ecosystem.

There are clear benefits to EMV SRC, however stakeholders note that more consumer education is needed to increase adoption, and that consumers should still be able to choose between different digital payment models.

B. EMVCo 3-Domain Secure (EMV 3DS)

The U.S. adoption of strong customer authentication (SCA) solutions, including EMV 3DS, lags behind European adoption. Europe requires SCA under PSD2, which will be effective in early 2021 for all European payments.[73] In addition to EMV 3DS, other solutions can be used to satisfy the SCA requirement under PSD2 in Europe. These include Apple Pay, using biometrics (e.g., Face ID or Touch ID) and Google Pay.

PSD2's goal is to allocate liability to the party at fault. A merchant/acquirer is liable for fraud if it does not apply SCA to the transaction (e.g., if it uses an exemption). If the merchant applies SCA, the issuer is liable for an unauthorized transaction, unless it can show that the cardholder acted fraudulently or with gross negligence (in which case, liability transfers to the cardholder).

In the U.S., EMV 3DS is not legally mandated, however the card network rules will shift liability for fraudulent transactions from the merchants to the issuers in early 2021. Until then, if a merchant is ready to implement and support EMV 3DS but the issuer is not, the merchant still owns the transaction liability if fraud occurs. Most U.S. stakeholders are waiting for the U.S. liability shift to occur and for the European mandate to become effective in early 2021. Merchant acquirers have not seen much demand from their clients, but some merchants are moving forward with EMV 3DS adoption.[74]

Card Network Perspectives on EMV 3DS

The card networks reported an increase in EMV 3DS authentication volume in April and May 2020, as more consumers shopped online because of the global pandemic. In the U.S., payment networks anticipate that over 95 percent of EMV 3DS authentication requests may result in a frictionless consumer experience (i.e., no step-up) because of the ACS risk-based authentication process. As EMV 3DS adoption expands in the U.S. and other countries, additional transaction statistics (based on

[73] Compliance was originally scheduled for September 2019 but was delayed to early 2021 because of technical challenges around biometric requirements for authentication.

[74] This information is based on interviews with key industry stakeholders, including card networks, responsible for the rollout of EMV 3DS.

over 150 data elements that can be used) will provide valuable insights for issuers that can result in higher approval rates and less fraud.

The card networks are pairing merchants and issuers to demonstrate the overall value of EMV 3DS for both stakeholders, including assurance and liability protection, and the ability for merchants to decide whether to enable EMV 3DS in their own secure environment.

Issuer Perspectives on EMV 3DS

The widespread adoption of EMV 3DS centers on issuers wanting to reduce e-commerce fraud. It has additional value because of its interoperability with EMV SRC and EMV tokenization. Although many large U.S. issuers have completed their 3DS implementations, some are in the process and others are taking a "wait-and-see" approach. Some issuers may have recently shifted their priorities because of the global pandemic and opportunities to learn from European adoption challenges.

With help from the card networks, issuers can use EMV 3DS to match authentication and authorization requests dynamically to determine what happened with the authentication and use the information to improve authorization rates.

In phase one, issuers must determine what is needed to comply with EMV 3DS and launch with merchants. In phase two, issuers must determine how to differentiate their services based on the additional data they include in the EMV 3DS message. Most large issuers will develop proprietary models to support EMV 3DS that improve upon their existing authentication models. Other issuers may use a third-party provider, card network, or both, to perform risk-based authentication, i.e., decline, step-up or approve the transaction.[75]

Smaller issuers may want to adopt EMV 3DS but lack resources to support implementation, including a dedicated risk team or outsourcing capability. Some issuers prefer to default every transaction to EMV 3DS, instead of performing their own risk analysis to determine if the transaction needs further review. Third- party providers offer this automatic default authorization.

Larger issuers can dedicate expert teams to develop risk models and augment them with additional risk decisioning tools. Many smaller issuers cannot develop those decisioning tools and rely solely on EMV 3DS through the card network or an ACS. For example, the issuer may receive approvals for all authentications and authorizations but receive a decline for an authorization from the ACS. If the issuer lacks resources to review every transaction, they cannot quickly respond to transactions that require step-up authentication and must default to EMV 3DS. For smaller to mid-sized issuers, developing a step-up process is challenging. They must

[75] The card networks and core processors offer neural networks to smaller and mid-sized issuers to help with fraud investigation and analysis of transaction volume. Issuers can rely solely on this option or build an internal solution to augment their use of these other solutions.

build the capability, usually by adding the functionality to request an OTP (one-time passcode)[76] from the consumer.

While EMV 3DS offers over 150 data elements, most authentication providers use only a subset to provide the same three responses (e.g., accept, review, or decline). Over time providers and issuers will fine-tune their use of the data and align it with their fraud models and risk infrastructure to improve authentication. The 3DS protocol mandates sending some data fields, but the majority are optional, so issuers are still developing their respective authentication models to leverage the broader data set. Issuers are likely to rely on as much data as possible to inform their risk decisioning. Some issuers anticipate this capability in early 2021, as most are working towards full adoption because of the approaching liability shift. Processors can help issuers with the data and building a customized risk model.

Using EMV 3DS for step-up authentication disrupts the transaction flow and consumer experience. According to some stakeholders, up to 16 percent of step-up transactions are abandoned due to the interruption. European businesses and issuers avoid friction by exempting transactions under 50 euros (approximately US$60) and granting a risk exemption to merchants that designate low-risk transactions (e.g., buying flowers).

Some issuers receive more reports from the card networks to help them identify false positives and understand if they are actually mitigating fraud through EMV 3DS. Issuers can generate and analyze transaction reports for disputes, but, overall, there is a gap in the timeliness and information received in daily reports from the networks.

Issuers are very concerned about account takeover (ATO) fraud, which is a significant cost for the industry. Some issuers expect to have a higher rate of ATO fraud without EMV 3DS adoption. Most large issuers acknowledge that EMV 3DS will improve security and address ATO fraud by making it more difficult for fraudsters to use stolen payment credentials. In Europe, issuers have also provided clear consumer messaging and education around ATO fraud to try to prevent it.

U.S. issuers can learn from their counterparts in Europe which took responsibility for EMV 3DS industry education. For example, European issuers informed consumers that they would receive periodic information about e-commerce transactions. While each country had its own implementation program, some organizations collaborated. In Belgium, several PSPs and issuers partnered around implementation and key challenges to identify the best path to adoption. U.S. issuers should also seek ways to collaborate with merchants and card networks to develop EMV 3DS messaging and education for consumers.

[76] One small issuer noted that building the OTP process requires designing screens and updating customer mobile phone numbers to align with the cardholders' payment cards to support "short codes."

Merchant Perspectives on EMV 3DS

U.S. merchant participation in the early version of 3DS 1.0 was low. As of November 2020, only a few merchants have begun to implement and operationalize EMV 3DS with the card networks. Many merchants acknowledge the value in obtaining more customer information in the EMV 3DS message provided to the issuer to perform authentication, but there are still challenges to address.

A key challenge is that some merchants only send their riskiest transactions through EMV 3DS because of the cost. Larger merchants typically send all their transactions through EMV 3DS and have developed proprietary fraud solutions to augment the EMV 3DS authentication, but to benefit the broader payments ecosystem, they need all the transactions to create a comprehensive database. When merchants only send a small percentage of their transaction volume through EMV 3DS, its skews the risk models for the entire ecosystem.

Merchants determine how many data fields they want to pass to the issuer in the EMV 3DS message. This requires considerable development to define the EMV 3DS dataset, based on the required and optional fields in the specification. Some merchants will never provide the optional fields. Others rely on issuers to define what additional data is optimal for their risk management models. A merchant interviewee shared that they selected between 20 to 25 data fields (from over 150 data fields available in the specification) and that creating the data subset was not resource intensive. However, one card network needed additional data for settlement, which did require more development. Ultimately, merchants want to know that their efforts will increase transaction approval rates before investing in resources to add data fields.

Merchants also raised concerns that issuers might use their data to competitively disadvantage them. For example, merchants will not share SKU-level data, which would allow issuers to potentially view certain products as high-risk. Issuers will need to justify their requests for more optional data and demonstrate how providing that data will benefit the merchant. Merchants should work with their acquirers to understand how EMV 3DS keeps data confidential and ensures that the data is only used for fraud prevention. A review of data confidentiality agreements with all parties should be a best practice.

While merchants see decreased fraud, they cannot discern if it is attributable to EMV 3DS because the networks do not offer reports or other tools to analyze the results (a similar concern among issuers). For example, the merchant never knows if an authenticated EMV 3DS transaction ultimately ends up as fraud, because the issuer bears the liability. Yet this would be valuable data to input to a merchant's fraud rules for risk-based decisioning. Merchants want to be able to pull key data from the EMV 3DS system to help mitigate fraud in their proprietary systems.

While the step-up authentication challenge percentages are relatively low, merchants want more data to confirm the numbers with a goal to achieve no more than 1 percent of transactions requiring step-up authentication.

For smaller and mid-sized merchants experiencing higher remote shopping due to COVID-19 or shifting their businesses online, EMV 3DS may be worth consideration. If the merchant previously supported 3DS 1.0, the card networks provide EMV 3DS and risk decisioning on their behalf. Merchants that also implemented EMV tokenization may gain additional value from EMV 3DS.

Interviewees expect EMV 3DS to show an 85 percent reduction in checkout times and a 70 percent reduction in shopping cart abandonment, resulting in increased sales conversions. EMV 3DS can also reduce false-positives that can be triggered by fraud prevention software, resulting in less lost revenue due to negative customer experience.[77] Finally, many merchants are working with the Merchant Advisory Group[78] to identify key challenges with EMV 3DS adoption, including debit routing.

Acquirer/Processor Perspectives on EMV 3DS

Acquirers and processors report that most of the merchants they support have not yet requested EMV 3DS because they do not yet have a compelling business reason to adopt it. However, they urge merchants to consider the growing e-commerce market as a valid business reason to adopt EMV 3DS to reduce fraud and increase transaction authorization rates.

Smaller to mid-sized banks and credit unions need their acquirers/processors to help implement EMV 3DS because the increased data that can be passed in the 3DS transaction represents a significant development challenge for them. Also, some banks and credit unions use one company for authentication services and another for authorization services, which means their acquirer/processor must authenticate a larger number of EMV 3DS transactions on their behalf. Until all issuers send 3DS messages in the latest format with the new data elements, merchants cannot take full advantage of this security protocol.

Community banks, in particular, tend to be concentrated in more regional areas of the country. The remote nature of these institutions creates challenges in terms of being able to obtain good and reliable customer mobile phone numbers and email addresses, which also impacts digital wallet adoption. Customers in regional areas are often still reluctant to share this information with their financial institutions.

Larger companies and card networks are benefitting from the additional data supported by EMV 3DS to reduce e-commerce fraud. However, most issuers and merchants are still developing their respective fraud and authentication models to use the broader data set. Issuers will probably rely on as much data as possible to inform their risk decisioning, but this capability will not be available until sometime in 2021.

---

[77] Payments Journal (2019, March 7). How 3D Secure 2.0 is set to be a game changer. *Payments Journal*. https://www.paymentsjournal.com/what-is-3d-secure-2-0-and-how-does-it-benefit-us/. Data made available by Visa.

[78] See https://www.merchantadvisorygroup.org/.

Acquirers and processors can help small and mid-sized FIs and merchants build customized risk models.

Digital Wallet Perspectives on EMV 3DS

Digital wallet providers are concerned EMV 3DS may become the default industry solution for applying SCA, despite the availability of other options. Card network rules cover scenarios where potential fraud or attempted fraudulent transactions create liability for the responsible stakeholder (e.g., issuer or merchant) to refund or compensate the consumer. A key benefit of applying SCA is that the liability that arises from a chargeback shifts from the merchant back to the card issuer for a transaction disputed by the consumer. These rules, when applied in a non-discriminatory manner, ensure that the payments ecosystem functions in a fair and transparent way for all participants while affording protection to consumers. Digital wallet providers are concerned that this will not happen in practice and prefer to see a liability shift that benefits merchants for also using alternative checkout methods, such as mobile/digital wallets.

C. W3C WebAuthn and Payment Request/Payment Handler APIs

W3C APIs are building blocks that help web developers create webpages that work consistently across browsers. The Payment Request/Payment Handler APIs eliminate the cumbersome online forms that consumers fill out to make purchases. The API sends the same data to the merchant in a different building block tailored to the payment method. When a merchant places a call to the Payment Request API, the merchant presents the payment methods they support to obtain payment data. The browser can respond or enable the consumer to answer the request (e.g., sending the merchant payment request via the mobile app). W3C is payment-agnostic, but the apps must establish a browser connection. The EMV SRC spec can leverage the W3C building blocks (e.g., Payment Request/Handler, and WebAuthn APIs) to help with the browser experience.

The WebAuthn/FIDO2 specification allows merchants to recognize the browser that a customer uses for online shopping and checkout. Most browsers and mobile phones now support the specification with biometric authenticators, making it ubiquitous.

The W3C APIs work with Chrome, Safari, Edge, and Samsung browsers. Over the last year, W3C has tried to increase merchant participation and customer adoption. Chrome currently has more API activity because it has a sufficiently large market, and because the APIs do not work with all browsers (e.g., Safari supports Apple Pay but no third-party payment apps).

W3C is also developing a Secure Payment Confirmation (SPC) specification to improve strong customer authentication. The specification combines all the W3C APIs for optimization. For example, SPC plans to use the Payment Request API to add a streamlined FIDO authentication to the payment flow to reduce the number of clicks in a session. Stripe is piloting SPC with Chrome to compare EMV 3DS step-up

authentication that uses OTP to FIDO authentication. The goal of the pilot is to demonstrate that consumers prefer WebAuthn over OTP for step-up. If the pilot supports this hypothesis, the Web Payments Working Group will formalize SPC to streamline authentication for multiple payment methods.

Card Network Perspectives on W3C

The card networks consider the W3C APIs complementary and interoperable with EMVCo specifications, and that W3C and FIDO technologies offer "under the hood" tools for EMVCo solutions. They participate in the W3C workgroup but have different API strategies. For example, one network is experimenting with the Payment Handler API, which could serve as an SRCi and open a Java Script window to present the Candidate List of payment cards to the consumer.

Issuer Perspectives on W3C

Issuers observed that W3C protocols currently lack sufficient industry engagement for large-scale adoption because payment stakeholders are focused on implementing EMV SRC and/or EMV 3DS. Many issuers have not evaluated WebAuthn/FIDO2 as an authentication solution or understand its full value because they have solutions that support device fingerprinting and device authentication to determine if a customer's credentials link to their device. Furthermore, if the API tokenizes transactions, they assume it follows the card network model.

Issuers also expressed uncertainty about whether W3C's Payment Request API will be able to change online customer behavior and gain traction in the market. Potentially, a future solution by a large technology provider could render this API obsolete.

Merchant Perspectives on W3C

Merchants generally understand that the Payment Request API initiates the browser payment and that the browser coordinates with all parties involved in a transaction to transfer payment information. Merchants want solutions that eliminate confusion and provide a connected commerce experience for the consumer. Like issuers, they want to shift away from the "NASCAR effect" that displays multiple payment buttons. They believe that some FIDO and W3C technologies support this need. For example, using WebAuthn may enable a merchant to know which browser a consumer tends to use for online shopping and checkout.

Acquirer and Processor Perspectives on W3C

Acquirers and processors view the Payment Request API as a way to allow the browser to store consumer payment credentials. The API reviews the available Payment Handlers and obtains the payment credentials from the user to send to the PSP. The Google Play app store is an example of how this works globally using the Payment Request API.

D. FIDO Alliance

Card Network Perspectives on FIDO

According to the card networks, FIDO is interoperable with all EMVCo specifications – EMV SRC, EMV 3DS, and EMV tokenization. FIDO can also be leveraged by online banking, e-commerce apps, websites, and payments to authenticate users. Merchants can serve as the FIDO or WebAuthn relying party and leverage EMV 3DS to report FIDO authentication data to issuers, which helps them make more informed risk decisions. This data, along with other transaction details sent via the 3DS *Authentication Request* message, can minimize friction through RBA when the online payment is made. Although this method creates a lower assurance level (vs. an issuer-managed credential), it is an approach that can be more easily deployed at scale than issuer-managed FIDO authentication methods.[79]

Issuer Perspectives on FIDO

Many issuers that accept Face ID on Apple devices apply FIDO authentication, which supports biometric solution providers. They trust that enabling customers to authenticate to a mobile banking app with Face ID provides greater convenience and security because Apple stores the biometric in the secure element of the device. Other issuers are comfortable enabling fingerprint verification, but not Face ID, on Samsung devices. Regardless of how FIDO is applied, the issuer must still secure its mobile banking app. Finally, issuers also benefit from FIDO authentication because it can reduce customer friction by eliminating the need for OTP.

Acquirer and Processor Perspectives on FIDO

The acquirer/processor perspectives on FIDO were covered in previous sections. Overall, acquirers and processors believe that WebAuthn has been the most interesting FIDO development. FIDO has always supported on-device authenticators for mobile devices (FIDO UAF), but WebAuthn extends FIDO to utilize on-device authenticators with mobile and desktop browsers.

IV. Key Messages and Recommendations

Over the last 10 years, the MPIW has focused on the challenges and opportunities to consumer mobile payment adoption in the U.S. The current payments environment is characterized by innovation and change, resulting in the expansion of available mobile/digital payment methods and more consumer payment choice. Furthermore, 55 percent of U.S. shoppers consider the mobile phone as the most efficient way to complete a purchase. However, security has been an underlying concern for protecting mobile/digital payments. According to the *Mobile Payment Authentication & Data Security 2019-2024 study*, biometric authentication is expected to increase by

[79] FIDO Alliance (2020, Sept 29). *Technical Note: FIDO authentication and EMV 3-D Secure – Using FIDO for payment authentication*.

over 1000 percent by 2024 to $2.5 trillion in transactions. In 2019, $228 billion in transactions already relied on this technology. As e-commerce and m-commerce transaction volumes grow, digital retailers will need to factor security into their payment strategies, along with flexible payment options and streamlined checkout processes.[80]

In light of these trends, various payment organizations and industry stakeholders seek to develop solutions to streamline the online consumer shopping experience and enhance security with stronger consumer authentication. EMVCo, FIDO Alliance, and W3C have developed protocols with strong value propositions for the payments industry. Industry stakeholders participating in these groups recognize the need for collaboration to make these protocols compatible for the payment ecosystem. Payments industry support and collaboration are needed to develop improvements to these specifications, build awareness, and provide broad industry education to increase adoption. Furthermore, some challenges need to be addressed in the near term, such as the ability for all stakeholders to generate informative reports based on their use of the additional data to help determine how the protocols impact fraud, authorization rates, and the customer experience.

In addition to these specifications, stakeholders recognize that other solutions exist, such as those provided by digital wallet providers. The solutions are equally important to the goal of reducing e-commerce fraud and enhancing authentication. No single solution is expected to prevail, allowing room for multiple options, as long as the consumer experience is addressed.

COVID-19 has also changed consumer perceptions of online security. According to a *2020 Experian Global Insights* report,[81] 53 percent of U.S. consumers expect more security steps when they shop online, and 48 percent expect to have more visible security measures in place on websites. Consumers not only have higher expectations when it comes to online security, but they also expect their digital transactions to be faster and more convenient. Experian's report found that one in three consumers are only willing to wait 30 seconds before they abandon an online transaction, a sign that businesses need to invest more in providing quick, convenient and secure transactions. A changing landscape means businesses must look for new ways to keep up with customer expectations. According to Experian's report, "strengthening the security of mobile and digital channels" was cited as the second-most important initiative that has been accelerated by COVID-19 among U.S. FIs, payment providers, and merchants.

Many significant technology changes are occurring to support stronger, more secure authentication while reducing customer friction in the shopping experience. Simultaneously, the industry is modernizing the financial services infrastructure

---

[80] Paterson, B. (2020, Dec. 29). 6 mobile payment trends here to stay. *Retail Customer Experience*. https://www.retailcustomerexperience.com/blogs/6-mobile-payment-trends-here-to-stay/.

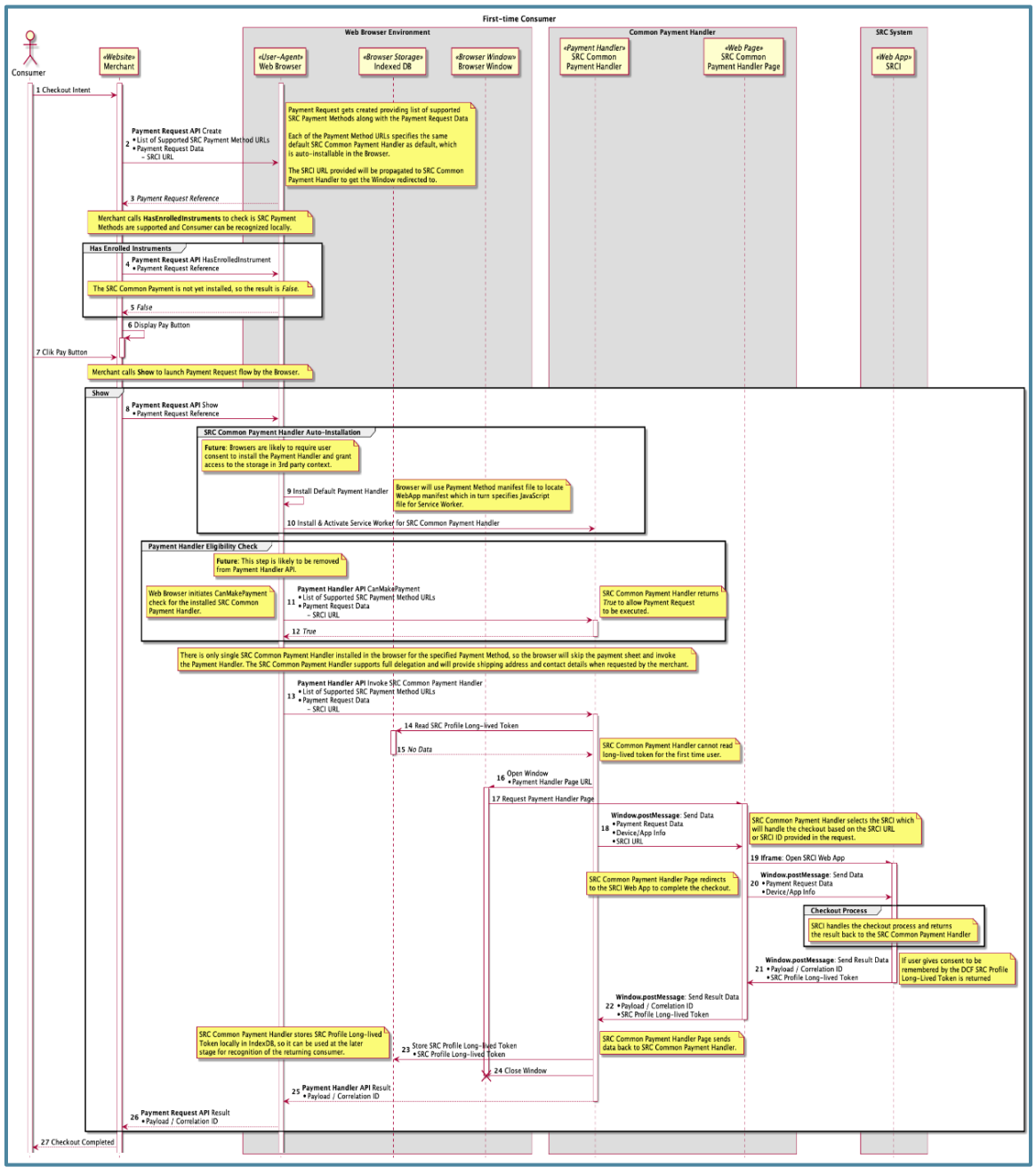
[81] Peters, K. (2020, Dec. 23). Adapting your fraud strategy to meet customer expectations. *Security solutions for enabling and assuring business*.

through open banking and API strategies that will enhance services available to consumers and offer them more control over their financial data.[82] The next few years will show which technologies and protocols succeed by offering strong security along with convenience and a good customer experience. It is likely that customer dependence on digital channels will become the norm, which means that security protocols such as EMV 3DS and FIDO authentication will be needed.

Streamlined and more secure online checkout experiences are a requirement for mobile and e-commerce payments. Whether the consumer uses a mobile app, digital wallet, or other payment method, the payments industry needs to offer more convenience for customers and improved conversion for merchants. The industry also needs to provide trusted platforms that protect the consumer's identity, payment credentials, and personal information. Industry stakeholders should collaborate to provide these deliverables to ensure that common industry protocols are aligned, interoperable, and scalable.

[82] Pandy, Susan. (2021, February). Modernizing U.S. Financial Services with Open Banking and APIs - Federal Reserve Bank of Boston (bostonfed.org).

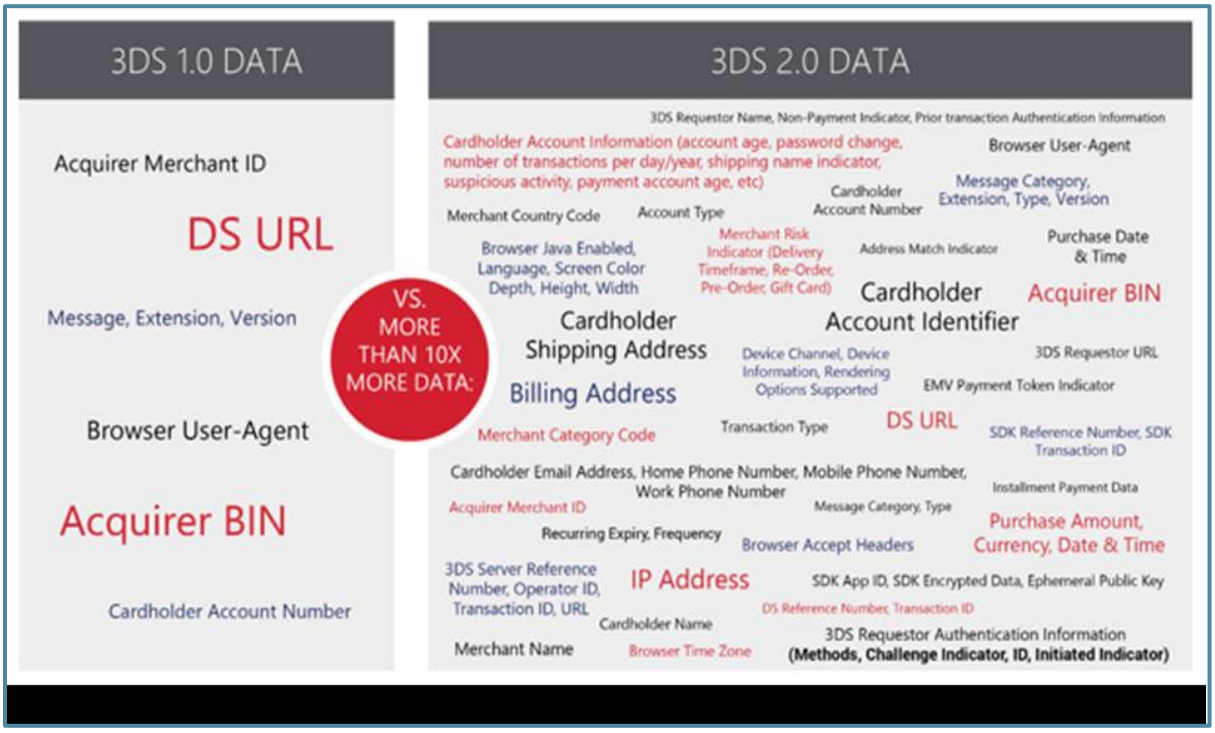
Appendix A: EMV 3DS, EMV SRC & W3C Payment Request Integration Scenario – 1st-time User Enrollment[83]



[83] Permission granted from Ian Jacobs, W3C. February 9, 2021. See https://github.com/w3c/src/wiki/SRC-Common-Payment-Handler-Concept.

Appendix B: EMV 3DS Enhanced Data Elements Compared to 3DS 1.0

The comparison shows differences between 3DS 1.0. Data and EMV 3DS Data collected by Merchants and the 3DS Server.[84]



[84] Visa Inc. (2019) as cited in U.S. Payments Forum. (2020, March). *EMV 3-D Secure Version 1.* https://www.uspaymentsforum.org/wp-content/uploads/2020/03/EMV-3DS-WP-FINAL-March-2020.pdf. Permission granted by Visa to use this figure on February 16, 2021.

Appendix C: EMVCo, FIDO, and W3C Publications

- EMVCo (2020). *FIDO Authentication and EMV 3-D Secure: Reducing Fraud and Friction for Online Payments*.
- EMVCo (2020, Oct. 8). *EMV 3-D Secure Use of FIDO Data in 3-D Secure Messages. Version 1.0.*
- EMVCo (2020, Nov. 5). *EMVCo, FIDO Alliance and W3C Collaborate on Educational Resource for More Secure and Convenient Web Payments*.
- FIDO Alliance. (2020, Sept). *FIDO Authentication and EMV 3-D Secure: Using FIDO for Payment Authentication*
- U.S. Payments Forum (2020, March). *EMV 3-D Secure*.
- Web Payments Security Interest Group (W3C, EMVCo and FIDO Alliance) (2020, Nov. 5) *How EMVCo, FIDO, and W3C Technologies Relate*.