FEDERAL RESERVE
BANK OF BOSTON™

Industry Perspectives on the Evolution of EMV Payment Tokenization

Revised May 6, 2019
[Original release date September 24, 2018]

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

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 Banks of Boston or the Federal Reserve System.

Mention or display of a trademark, proprietary product or firm in this report does not constitute an endorsement or criticism by the Federal Reserve Bank of Boston or the Federal Reserve System and does not imply approval to the exclusion of other suitable products or firms.

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

Table of Contents

Executive Summary

In 2014, the introduction of technical specifications for end-to-end *payment tokenization* transformed the ability to secure mobile and digital transactions throughout the payment transaction flow with the release of the *EMV Payment Tokenisation Specification – Technical Framework Version 1.0* (EMV v.1.0).[1] EMVCo published an updated version *EMV Payment Tokenisation Specification — Technical Framework Version 2.0* (EMV v2.0)[2] in 2017. This whitepaper examines the changes in payment tokenization since its introduction and impacts to the payments industry. The research represents the authors' views with input from Mobile Payment Industry Workgroup (MPIW)[3] members and qualitative interviews with key industry stakeholders.[4]

The increased adoption of payment tokenization since 2014 has positively impacted issuers who have reported increased authorization approval rates and lifecycle management by enabling them to collect more information about the token requestor (TR).[5] The ecosystem now includes third party[6] token service providers (TSPs),[7] which can help businesses achieve scale by extending payment tokenization to the online/card-on-file (CoF)[8] environment without needing to integrate with multiple card networks. Payment tokenization is also considered a key tool for mitigating risk in the CoF channel by eliminating the need to store and transmit a customer's primary account number (PAN).[9] Despite advancements in security made with payment tokenization, challenges remain for merchants to be able to reconcile the underlying PAN with the token for customer service functions, such as returns. Stakeholders are also monitoring how payment tokenization will be applied in a connected device environment (e.g., Internet of Things (IoT) and wearables technology).

While this paper is focused on payment tokenization, merchants have used security tokenization for many years to protect their customer payment account data. Historically, *security tokenization*[10] in the payments industry was and still is primarily applied by merchants, acquirers, and technology providers to protect data-at-rest, such as CoF systems for repeat remote transactions. Security tokenization eliminates sensitive

[1] EMVCo (2014, March). *EMV Payment Tokenisation Specification – Technical Framework Version 1.0.* Available at https://www.emvco.com/terms-of-use/?u=wp-content/uploads/documents/EMVCo_Payment_Tokenisation_Specification_Technical_Framework_v1.0.pdf.

[2] EMVCo (2017, Sept). *EMV Payment Tokenisation Specification – Technical Framework Version 2.0*. Available at https://www.emvco.com/terms-of-use/?u=wp-content/uploads/documents/EMVCo-Payment-Tokenisation-Specification-Technical-Framework-v2.0-1.pdf.

[3] For a list of MPIW member organizations, see http://www.bostonfed.org/bankinfo/payment-strategies/mpiw/index.htm.

[4] Industry stakeholders include financial institutions, merchants, card networks, acquirers, payment processors, technology providers, payment network operators, and industry associations.

[5] 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 applications, web browsers, card issuers, merchants, acquirers, acquirer processors, and payment gateways). TRs must register and comply with a TSP's proprietary requirements, receive a token requestor ID, and 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 (e.g., host card emulation).

[6] This paper uses the term "third party" to refer to TSPs that are non-networks. Third party TSP is not an EMV defined term. Any TSP that support EMV payment tokens needs to operate in accordance within the procedures of the Token Programme policy they are supporting.

[7] The *EMV Payment Tokenisation Specification Technical Framework* defines a token service provider as a role within the payment tokenization ecosystem that is authorized by a Token Program to provide payment tokens to registered token requestors (e.g., merchants, wallet providers).

[8] Card-on-file (CoF) refers to the authorized storage of a consumer's payment credentials by a merchant, payment service provider, or wallet service provider that allows the consumer to conveniently make repeat or automatic purchases without the need to re-enter payment credentials each time.

[9] The primary account number (PAN) is a number printed on the plastic credit or debit card and contained on the card's magnetic stripe and in the card's microchip. It identifies the card issuer and the cardholder account. The number is 15-19 digits and includes a check digit as part of the authentication.

[10] A method for protecting payment card data post-authorization or for data-at-rest by substitution of a sensitive payment credential information (i.e., PAN) with a unique, randomly generated sequence of numeric and/or alphabetical characters. Also referred to as *acquirer tokenization* because it is supplied by acquirers to merchants, or can be supplied by third party technology providers and payment gateways. Some merchants may develop their own proprietary systems.

card data from their systems and reduces the financial and reputational risks to the industry associated with data breach. As data breaches and other card-related compromises have increased, there is need to utilize a variety of solutions that secure payments data from end-to-end has grown, particularly for card-not-present (CNP)[11] payment forms such as e-commerce and mobile payments.

Expanding payment tokenization into the e-commerce channel could benefit the industry in terms of reducing fraud by applying a consistent key security method across payment channels. Interoperable standards will also play a pivotal role in driving ubiquitous security in e-commerce. However, the expanded use of payment tokenization across use cases and channels will result in consumers having more tokens in multiples places (e.g., CoF, e-commerce websites, or digital wallets). Industry collaboration is needed to educate consumers on how and where their payment credentials/tokens are stored and secured in the mobile/digital environment. Finally, as payment tokenization continues to expand, the industry must anticipate future innovations for securing mobile and digital payments and evaluate whether or not tokenization will be enough to secure the payments environment for the foreseeable future.

Acknowledging different industry views, our goal is to encourage further collaboration among stakeholders to resolve differences to the mutual satisfaction of the industry and provide optimal solutions and options for consumers and businesses.

I. Introduction

The MPIW was established in January 2010 by the Federal Reserve Banks of Boston and Atlanta. This thought leadership group meets several times a year to share information and ideas, and discuss the barriers and opportunities in retail mobile payments, with a shared goal of building an efficient, secure, and ubiquitous mobile payments environment in the U.S. As the mobile payments environment has evolved to encompass new technology platforms and solutions, channels, and participants to drive changes in consumer payments behavior, the MPIW has modified its objectives.

In recent years, improving the security of the remote payments environment has been a focus among industry stakeholders. The migration to EMV chip cards reduced counterfeit payment card fraud at the point-of-sale (POS) but shifted fraud to the e-commerce channel, where new or enhanced fraud prevention tools are needed. Payment tokenization of card credentials, initially used to mitigate fraud for near-field communication (NFC)[12] mobile POS and in-app purchases made through Pay wallets (e.g., Apple Pay, Google Pay, and Samsung Pay), is now being used to help reduce e-commerce fraud. Accordingly, the MPIW formed a subgroup in 2017 to understand how payment tokenization has evolved over the last three years and how it will be used to complement efforts to improve security in the e-commerce channel.[13] Analysis included a review of EMV v2.0, industry research, and stakeholder interviews with issuers, card networks, merchants, processors, and other non-bank technology providers. Their perspectives helped to

[11] Card-not-present is a payment made for a purchase using a payment card, where the cardholder/card is not physically present to allow the merchant to validate the cardholder at the time of purchase (e.g., by U.S. postal mail, telephone, or internet).

[12] Near field communication (NFC) is a standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart. NFC-enabled mobile phones incorporate a smart chip (secure element) that allows the phone to store the payment app and consumer account information securely and use the information as a virtual payment card.

[13] This analysis builds on work completed in 2015, which resulted in the publication, *Is Payment Tokenization Ready for Primetime? Perspectives from Industry Stakeholders on the Tokenization Landscape*. Crowe, M. and Pandy, S., et al. (2015). The original report explained the different industry approaches to tokenization – security or acquirer tokenization and payment tokenization (i.e., network tokenization).

inform current stakeholder and market issues, challenges and opportunities, and to identify potential knowledge gaps and recommended solutions.
Key issues assessed include topics that required further clarification and/or education:

1. Changes between EMV v1.0 and v2.0
2. Emergence of third party TSPs and supporting requirements
3. Expansion of payment tokenization to e-commerce and CoF use cases
4. Industry perspectives and implementation plans for the Payment Account Reference (PAR) number
5. Implications of payment tokenization for IoT and wearables technology

II. Changes between EMV Payment Tokenisation Specification v1.0 and v2.0

The original *EMV Payment Tokenisation Specification Technical Framework* (EMV v1.0) presented a high level technical framework that introduced the payment token, a value that is generated during the mobile wallet enrollment process to replace the PAN when the consumer initiates a payment transaction.

The framework also defined the roles of key participants engaged in tokenizing card-based mobile payments. As authorized by the issuer, the TSP generates and maps the token to the PAN and provides additional security functions such as token domain restriction controls[14] to ensure appropriate use of the payment token. The merchant accepts the token in lieu of the PAN to process the payment. The token maps back to the PAN stored in the TSP's token vault to enable authorization by the card issuer. Since the merchant does not use or store the cardholder's PAN, in the event of a compromise, a fraudster would only obtain the payment token and associated transactional data. A dynamic cryptogram may be generated for each transaction; therefore, preventing replay of the transaction message if the payment token data is intercepted or breached.

The *EMV Payment Tokenisation Specification Technical Framework v2.0* was updated to support the global expansion of payment tokenization and to achieve scale by elaborating on the specific functions of the entities involved in the token process. Some of the key changes include the expansion of the TSP role and functions, and a PAR whitepaper was released to provide more understanding of PAR, which was introduced in *EMV Specification Bulletin No. 167*.[15]

Token Service Providers

When EMVCo[16] published the first tokenization specification v1.0, the only TSPs in the U.S. were the major card networks (Visa, Mastercard, American Express, and Discover), which allowed for a tightly controlled and secure process. Since then, other entities have expressed interest in becoming TSPs in the U.S. and EMV v2.0 introduced the "Token Programme," which defines policies that govern activities for

[14] Token domain restriction controls are parameters established as part of payment token issuance by the TSP that allow for enforcing appropriate usage of the payment token in payment transactions. Examples include use of the payment token: 1) with particular presentment modes (e.g., contactless or e-commerce); 2) at a particular merchant that can be uniquely identified; and 3) verification of the presence of a token cryptogram that is unique to each transaction.

[15] EMVCo. (2016, Jan., 1st Ed). *EMV Specification Bulletin No. 167: Payment Account Reference (PAR)* (Spec Change). Available at http://legacy.emvco.com/specifications.aspx?id=23.

[16] EMVCo is a consortium that manages the security specifications for chip-based payment cards (EMV), including payments tokenization and the 3DS authentication protocol. It is jointly owned by American Express, Discover, Visa, Mastercard, JCB, and Union Pay.

TSPs to follow. Where EMV v1.0 provided a basic overview of TSP functions, EMV v2.0 takes a more granular approach and provides more details on each TSP function:

- Mapping payment tokens and token expiry dates to underlying PANs and PAN expiry dates
- Generating and issuing payment tokens to TRs, and de-tokenization
- Determination of token assurance methods to indicate the identification and verification (ID&V)[17] performed
- Establishing security requirements and controls related to the token vault, token provisioning, and token processing
- Establishing permissible token domain restriction controls
- Establishing requirements for payment token and PAN lifecycle management[18]
- Registration and approval of TRs and TSPs

EMV Payment Tokenisation Specification Technical Framework v2.0 elaborates on some of the v.10 descriptions of discrete TSP functions. Figure 1 lists a few of the original EMV v1.0 and revised v2.0 TSP functions.[19]

Figure 1. Comparison of TSP functions in EMV v1.0 versus v2.0

EMV Specification Version 1.0		EMV Specification Version 2.0
1	Ongoing maintenance and operation of a token vault	
2	Payment token generation and issuance	
3	Payment token provisioning	Token issuance and token provisioning, including facilitation of PAR field and PAR data in provisioning requests
4	Application of security and controls	
5	Token requestor registry functions	
6	De-tokenization and tokenization	
7	Application of token domain restriction controls	
		Recognition that the entity introducing payment tokenization to a payment ecosystem is responsible for establishing a payment token program. This program will define the business policies and processes for the generation, issuance and full lifecycle management of payment tokens to ensure their effective delivery.
		Additional detail on payment token processing which clarifies the use of a payment token in the authorization process.

[17] ID&V is a process performed by the card issuer during mobile wallet enrollment to ensure that the cardholder is legitimate before the cardholder's PAN is replaced with a payment token. EMV v2.0 modifies the ID&V process based on lessons learned from EMV v1.0 and revised the former token assurance level concept to represent a consistent value related to token assurance that is based on: (1) type and outcome of the ID&V process during provisioning; (2) entity performing ID&V; (3) domain in which the payment token is to be used; and (4) supporting token assurance data. The values assigned focus on the facts of "what" ID&V method was done and "who" (typically the issuer) performed the ID&V method, and are used to assign a risk score to the token.

[18] See §4 – Token Programme. *EMV Payment Tokenisation Specification – Technical Framework Version 2.0.*

[19] See §3.7 – Token Service Provider. *EMV Payment Tokenisation Specification – Technical Framework Version 2.0.*

		Introduction of new concepts around shared and limited use payment token to support the expansion of e-commerce use cases.
		Introduction of the payment token assurance method (replacing token assurance level) to enable a token requestor, such as an issuer, digital wallet provider or merchant, to have information available related to the identification and verification processes associated with the issuance of a payment token.

An EMVCo-registered TSP is not required to perform all of the TSP functions outlined in the specification. For example, a TSP may choose to only perform token provisioning and lifecycle management.

III. Impacts of Evolution of Payment Tokenization on the Mobile Payments Landscape

A. Emergence of Third Party Token Service Providers (TSPs)[20]

As noted above, EMV v1.0 did not address competitive options for third parties to become TSPs or provide their own TSP services, which industry stakeholders noted as a market gap in the 2015 tokenization report published by the Boston and Atlanta Federal Reserve Banks.[21] Businesses that seek to become TSPs must meet the requirements, including any certifications, set forth by the card networks. works. Some businesses that have become TSPs have demonstrated their commitment to security by adhering to the y Federal Information Processing Standards (FIPS),[22] as well as relevant industry standards (e.g., ISO 8583[23] and ISO 20022[24]). These businesses must demonstrate the ability to secure payment credentials within their token vault[25] if they choose to maintain and operate one (i.e., proprietary vault or outsourced).

Businesses must also adhere to the Payment Card Industry Security Standards Council's (PCI SSC)[26] *TSP Security Requirements (EMV Payment Tokens)* and *2016 Card Production and Provisioning Logical Security Requirements* version 2.0. Third party TSPs that choose to maintain and operate a token vault must also comply with the PCI Data Security Standard (PCI DSS).[27]

Third party TSPs are more common in other countries, particularly those that have independent domestic payment networks (e.g., Canada, Asia, South America, Europe, and Africa), where payment processing

[20] EMVCo does not define a "third party TSP." This is a term used throughout this paper to refer to a non-network TSP.

[21] Crowe, M. and Pandy, S., et al. (2015). *Is Payment Tokenization Ready for Primetime? Perspectives from Industry Stakeholders on the Tokenization Landscape*.

[22] FIPS are published by the National Institute of Standards and Technology (NIST) to address security and interoperability standards on federal government computer systems in areas that pre-existing federal laws and regulations do not address. FIPS mandates several types of security and auditing procedures that depend on the type of data being stored and protected. FIPS 140-2 covers cryptographic standards for securing sensitive non-confidential data and requires companies to implement security safeguards that conform.

[23] ISO 8583 – Financial transaction card originated messages – Interchange message specifications. ISO 8583 specifies a common interface by which financial transaction card-originated messages can be interchanged between acquirers and card issuers. It specifies message structure, format, content, data elements, and values for data elements. See https://www.iso.org/obp/ui/#iso:std:iso:8583:-1:ed-1:v1:en.

[24] ISO 20022 is a global and open methodology that can be followed when creating financial messaging standards. First published in 2004, ISO 20022 is widely recognized as the standard of the future.

[25] A token vault is a secured repository, or database, that handles token generation, issuance, and mapping (i.e., token to PAN mapping, re-mapping, de-tokenization) as well as lifecycle management of tokens and PANs, cryptographic processes to support tokenization functions (e.g., hardware security modules), and maintenance of domain restriction controls during transaction processing.

[26] The PCI Security Standards Council is an open global forum responsible for the development, management, education, and awareness of the PCI security standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements. For more information, see https://www.pcisecuritystandards.org.

[27] PCI DSS is an information security standard for organizations that handle branded credit cards from the major card schemes and was created to increase controls around cardholder data to reduce credit card fraud.

may occur outside of the major card networks. For example, Canada has agreements with the card networks for cross-border transactions. However, because its Interac debit network[28] provides a proprietary token, the card network tokenization model does not work for all issuers in foreign markets. This creates an opportunity for third party TSPs to offer more services than those in the U.S., such as serving as a switch for multiple TRs to route tokens between different TSPs.

Only a few specialized companies (e.g., core processors and digital security companies) may be able to meet the threshold to become certified TSPs in the U.S. Some digital security companies[29] already provide tokenization/TSP services in other countries but this ability is more complex in the U.S. where tokens from third party TSPs must still flow through the card networks. TSPs must have access to the PANs in order to provide the networks with a "mirror" token vault so that the networks can ensure the operation of their payment networks to the standards they ensure for their merchants, issuers, and the ecosystem.

Stakeholder Perspectives

Many stakeholders view the introduction of third party TSPs to the payments ecosystem as a way to achieve scale and expand tokenization to the CoF environment. Third party TSPs enable stakeholders to connect to a more centralized entity for token services rather than connecting separately to each card network.

Stakeholders are generally supportive of third party TSPs. Becoming a third party TSP is a strategic decision based on interests that may differ from the card networks. Third party TSPs create competition which drives innovation. While the *EMV Payment Tokenization Specification Technical Framework* is designed for card-based systems, some stakeholders may it to speculate its application to other use cases, such as real time payments (RTP), person-to-person (P2P), demand deposit account (DDA)/automated clearing house (ACH), and IoT, which may not be high priorities for card networks. Third party TSPs can help businesses achieve scale by extending tokenization to the online/CoF channel, enabling a merchant/TR to connect and obtain tokens associated with multiple card networks through one, third-party TSP, rather than through each card network TSP.

Merchants support more competition from third party TSPs and the opportunity to minimize the number of TSP connections for enhanced efficiency. Like other stakeholders, they agree that security must be paramount. Larger merchants with proprietary and/or acquirer-based security tokenization systems and backend token vaults would not need third party TSPs. Using proprietary systems, the acquirer/processor captures the customer's PAN for proximity and remote transactions and replaces it with a security token that is sent to the merchant and used for future authorizations.

[28] Interac is a cooperative venture among Canada's major financial institutions that operates a single shared debit network.
[29] Examples include Gemalto and Giesecke & Devrient.

Third Party TSPs Active in the U.S.

The Clearing House (TCH)

In October 2017, The Clearing House (TCH)[30] announced plans to launch a third party TSP in the U.S. for production in 2018. TCH plans to use a third party token vault and offer token provisioning and lifecycle management functions for its participating members. Initially, TCH will offer TSP services to member issuers that have not yet tokenized their portfolios. For example, TCH issuers of Mastercard-branded cards will have the option to tokenize their customer accounts through TCH. Furthermore, TCH issuers will only be able to connect to wallet providers (e.g., Apple Pay) through TCH.

TCH will operate the full token provisioning process for its members and serve as the intermediary between the parties to pass data needed to perform ID&V. The TCH token vault will maintain the cryptographic keys to manage the token-to-PAN mapping, and provide a mirror vault of that mapping (without domain restrictions and expiration dates) to each card network to update their own mirror vaults. The card networks will use the mapping only if needed to approve transactions when they cannot connect to an issuer to confirm that a PAN is valid.

First Data Corporation (FDC)

When Apple Pay launched in 2014, FDC offered its first tokenization service where it connected to the card network TSPs "on behalf of" its issuer clients to deliver token services to issuers.

In December 2017, FDC implemented its own TSP with Mastercard and Apple and plans to implement with Visa in the near future. FDC offers the following TSP services to its financial institution (FI) and merchant clients: 1) token vault that supports token-to-PAN mapping; 2) token provisioning; 3) lifecycle and risk management; 4) fraud management solution integration; and 5) private label card[31] integration.

FDC's rationale for becoming a third party TSP was to have more control over the tokenization process (e.g., creation, storage, issuance, and management) and to offer multiple options to its customers. This enables stakeholders to have one access point across multiple card networks and integration with multiple services. Third party TSPs may be able to reduce administrative and technical efforts for merchants; streamline integration and the number of interfaces that they maintain; and reduce the amount of code that merchants (or their providers) must develop – all necessary steps for a merchant to integrate with multiple card networks.

FDC has a trusted relationship with its large FI client base, for which it already securely stores and manages PANs. Therefore, vaulting a token does not represent a significant increase in risk to its business model, unlike a fintech or start-up company with limited financial services experience and less-established customer relationships.

[30] Established in 1853, TCH is the oldest banking association and payments company in the U.S. and is owned by twenty-four of largest U.S. leading commercial banks for which it provides payment, clearing, and settlement services.

[31] Private label credit cards (PLCC) are cards branded for a specific retailer, independent dealer, or manufacturer.

B. Expansion of Tokenization into E-Commerce

According to the U.S. Department of Commerce, e-commerce sales accounted for 9.6 percent of total retail sales in the second quarter of 2018.[32] While payment cards will continue to be used at POS, some stakeholders expect to see an increase in mobile browser, in-app, order ahead, and other related mobile CNP transactions, where implementation of security or payment tokenization is key to mitigating the shift in fraud and securing the CNP channel.

Recognizing the growth in account and transaction volume, and potential increase in e-commerce fraud, EMV v2.0 included changes to support tokenization for CNP uses cases. It explains how the dynamic cryptogram associated with the payment token is transmitted in the e-commerce channel for CoF merchants, which differs from mobile in-app transactions that are secured with a payment token bound to the mobile device that generates a dynamic cryptogram. However, remote use cases such as CoF or browser, which do not have a (mobile) device to bind the token and generate the cryptogram, are treated differently. *EMV Payment Tokenisation Specification Technical Framework v2.0* provides the ability for a token cryptogram to be optionally used for CoF. It does not discuss how or where the cryptogram originates, nor is it explicit placement in a transaction message as those decisions are outside of the specification scope.

The *EMV Payment Tokenisation Specification Technical Framework v2.0* serves as a toolkit for stakeholders to determine their own path of implementation. Stakeholders may determine whether or not to use a CVV or card verification code (CVC), but this will depend on how tokenization is overlaid into the system during implementation. Some TSPs may require the use of a cryptogram for an initial transaction, but not for subsequent ones. Other TSPs may not require any CVV or CVC.[33]

Stakeholder Perspectives

Stakeholders want to avoid exposing more accounts to fraud as e-commerce volume grows and CNP merchants proliferate. Issuers acknowledge that tokenizing Pay wallets addresses some of this fraud by reducing online exposure of the PAN, but CoF accounts remain at risk. While the largest issuers have implemented payment tokenization for POS and CoF, smaller banks and credit unions may not have the capability to support payment tokenization or have it on their roadmaps. Those undecided continue to monitor developments to determine the incremental benefits of tokenizing CoF accounts. Issuers also have to consider how to respond to the different card network approaches for implementing CoF tokenization. One network requires issuers that already offer POS tokenization services to expand payment tokenization to the CoF environment, while another network allows issuers to decide if they want to add CoF tokenization.

Some stakeholders expect more CNP merchants to implement payment tokenization over the next year. CNP merchants have two options: 1) accepting digital checkout wallets; and/or 2) tokenizing their CoF databases, including new and/or existing PANs.

[32] U.S. Census Bureau, Department of Commerce (2018, Aug. 17). *Quarterly retail e-commerce sales 2nd quarter 2018.* Retrieved from https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

[33] It should be noted that the card networks have different implementations for inserting dynamic data in transaction message fields.

To reduce the risk of cardholder PAN compromise in the e-commerce environment, card networks have added payment tokenization to their digital checkout wallets. To offer digital wallets to their customers, issuers must connect to each card network with which they issue cards. Merchants add the digital checkout button on the website or mobile app checkout screen. Once the customer is enrolled for the digital wallet, only the tokenized PAN flows through the CNP transaction payment process. However, often the customer must enter the PAN to enroll, creating a risk of exposure if that process is not adequately secured.

Replacing CoF PANs with payment tokens does not involve the customer's mobile device. If a CNP merchant decides to tokenize PANs that are stored in its CoF database, the merchant or its acquirer must enroll with the respective card network token service (e.g., Mastercard Digital Enablement Service or Visa Token Service). Once enrolled, the CNP merchant or its acquirer can request a payment token through the issuing FI the first time a customer uses the PAN for a payment. Some larger merchants are working independently or with their processor/acquirers to convert their new and existing CoF PANs to payment tokens, but many still remain undecided.

Payment tokenization for CoF databases can enhance security, particularly where no other tokenization methods are used, but merchant perspectives on key themes related to the expansion of tokenization to the e-commerce channel tend to differ. Generally, merchants agree that securing the e-commerce environment using tokenization has value, but want to be able to opt in or out with the CoF model, depending on the impact to transaction routing. They would like to process transactions in a way that is best suited for their respective business models and that supports interoperability.

Some franchised quick-service restaurants (QSRs) outsource management of their websites and remote commerce support to third party providers; therefore, if e-commerce transactions are tokenized then the overall operational impact to the QSR is minimal. However, integration with third party providers to manage their e-commerce sites can impact internal fraud tools (e.g., solutions that use a hash to identify the customer's payment card), particularly since multiple providers use the PAN on the backend to pass information about the transaction with each other. On the other hand, when a QSR relies on a payment token instead of the PAN, the communication is only two-way (between the TSP and the QSR) in the event the actual PAN is needed to resolve a transaction issue.

Payment processors are concerned that their workload and management responsibilities will expand exponentially as more CoF merchants or IoT manufacturers become TRs. These TRs must maintain a connection with each network TSP to request a token. Third party TSPs (e.g., issuer or processor) also need to contract separately with each TR. This added complexity may incent processors to offer "token aggregator" services on behalf of online merchants.

Use of payment tokenization is expected to increase as more CNP-type mobile payment use cases are implemented (e.g., for mobile apps) and as more consumer adopt mobile/digital payments. Mobile order ahead via a mobile app using a stored value card has become an important e-commerce component to several QSR businesses. Even merchants that receive their services from acquirers, who tokenize the data at rest using security tokens,[34] should consider using payment tokenization for CoF data. Use of security tokenization can still expose a merchant to potential data breaches if a PAN is compromised even in another

[34] Security tokens are sometimes referred to as acquirer tokens and enterprise tokenization models because they are merchant-centric. Payment tokens are also referred to as issuer or EMVCo tokens. For this paper we use "payment" and "security" tokens.

merchant system because the PAN can be used to attempt fraud across multiple merchants. It is in the industry's best interest for all merchants to leverage some type of tokenziation to avoid vulnerability to risk of PAN exposure.

Some stakeholders may not fully understand how payment tokenization secures CNP transactions. The PCI SSC, Accredited Standards Committee (ASC) X9,[35] and TCH noted the value of payment tokenization in different payment channels, but emphasized the need for education and awareness across all stakeholders, including consumers, in order to build adoption and to ensure proper implementation and use of payment tokens.

Stakeholders also raised questions about work by the World Wide Web Consortium (W3C)[36] to create browser standards with enhanced security for e-commerce. Released as a "candidate recommendation" in April of2018, the WebAuthn[37] standard provides a common way for browsers to accept fingerprint, facial, and other forms of biometric authentication from a smartphone, desktop, or USB-connected hardware, rather than passwords. It allows tokenized consumer payment information to be stored in the browser, enabling the consumer to select among several payment cards to complete a purchase and offer a more streamlined checkout experience. This information is included in the ISO 8583 message that is sent to the acquirer.

C. Payment Account Reference (PAR) Number

Merchants historically relied on the last four digits of the PAN for pre- or post-authorization purposes. Using the actual PAN to connect customer transaction behaviors enabled merchants to efficiently support value-added programs (e.g., loyalty, couponing, returns, chargebacks, transaction risk scoring, and regulatory compliance, such as anti-money laundering). Payment tokenization makes this process more complicated because the token (which replaces the PAN) often does not carry the same last four digits as the actual PAN.

Multiple payment tokens associated with a single PAN (e.g., shared PAN or PAN assigned to multiple form factors) further complicate the process. If a consumer uses the same PAN with one merchant to make a purchase with a Pay wallet, to pay online using CoF, or to pay with a digital checkout wallet, each instance utilizes a unique token linked to the same PAN. Because only the TSP sees the relationship between the PAN and the associated tokens, this scenario prevents merchants from being able to identify transactions at the aggregate cardholder level to monitor and analyze consumer behavior.

Below is an example of how the allocation of payment tokens at the device level may impact customer returns and other transactions as many merchants rely on the PAN:

[35] X9 is responsible for the industry standards for financial cryptography and data protection, including payment card PIN management, credit and debit card encryption, and related technologies and processes. ASC X9A Retail Payments Subcommittee recently released a 2018 Technical Report: *Card-Not-Present (CNP) Fraud Mitigation in the United States: Strategies for Preventing, Detecting, and Responding to a Growing Threat*, to educate industry stakeholders on the risks presented by criminal activity and how to more effectively prevent, detect, and manage CNP fraud.

[36] W3C standards define an Open Web Platform for application development that has the potential to enable developers to build interactive experiences, powered by vast data stores that are available on any device. See http://www.w3.org/standards/.

[37] WebAuthn was developed by the Fast Identity Online (FIDO) Alliance, a consortium of technology, financial and other companies. WebAuthn is the latest authentication standard from FIDO. The candidate recommendation phase prefaces final approval of a web standard.

- A customer returns a purchase without the original receipt, presents the payment card, and the merchant processes a non-receipted return. This creates a significant challenge for merchants with high return volumes, since they are unable to issue a credit back to the payment card account.

- A husband makes a purchase with his mobile phone which his wife returns without a receipt. She uses the same PAN provisioned to her mobile phone, which has a different token. As a result, the merchant cannot locate the transaction record and the link is broken between merchant and customer or transaction and customer. The merchant typically issues a store credit instead of a refund to the payment card.

- Tokenizing transit payments creates another challenge if the PAN is used to discount a fare. Therefore, this process would be altered if the PAN were replaced with a token.

The operational challenges of payment tokenization identified the need for an alternative to using the PAN as a customer identifier for non-payment functions. PAR associates all payment tokens linked to a single credit or debit PAN without the need to use the underlying account number. It is intended to eliminate the need for the PAN by providing a linkage to the PAN across different tokens, effectively becoming a key for correlation of tokens and PAN.

The TSP ensures that PAR is available for linkage to the underlying PAN, which cannot be reverse-engineered to reveal the payment token or PAN values. It can only be used for non-payment functions as noted above.

PAR implementation required collaboration between issuers and acquirers. The card networks set October of 2017 as a deadline for acquirers to have developed the capability to pass the PAR value to their merchant customers. To support this effort, the card networks established host testing requirements for issuing and acquiring processors, and for testing terminals that support PAR.

Stakeholder Perspectives

Industry stakeholders recognized the value of PAR and initially supported the concept. However, more recently, PAR has received mixed responses and interest appears to have declined. Several industry stakeholders, including merchants, issuers, processors, payment providers, and others were interviewed to obtain a collective perspective on PAR, but the segment most impacted and intended to benefit from PAR was the merchant.

In general, merchants find payment or security tokenization to be a valuable and practical solution and view PAR as a positive development given the number of tokens and PANs in the ecosystem. Prior to PAR, some merchants that implemented payment tokenization for the Pay wallets developed their own solutions, such as use of a customer's mobile phone number for loyalty programs or other backend functions.[38] PAR may resolve problems in the long-term, but many stakeholders agree that it will be a major, multi-year effort to implement, because merchants will need to apply the PAR everywhere tokens and PANS are used today to minimize business disruption. Other considerations include:

[38] Merchants that have not adopted Pay wallets and payment tokenization rely on a proprietary and/or acquirer token process to remove sensitive cardholder data from their payment environments.

1. Merchant investment to re-engineer systems to integrate PAR into all authorization and clearing messages. It should be noted that not all card networks and their acquiring processors may require inclusion of PAR in the transaction message.

2. Merchant and acquirer backend system upgrades to accept PAR as the new index for merchant loyalty programs and acquirer risk management. The PAR format and field length do not match the PAN (29 alphanumeric vs. 16 numeric characters) and merchant and acquirer systems currently support only numeric fields. Other systems that currently support a 16-digit PAN, including customer relationship management (CRM), would also need to be modified.

3. Build and maintain lookup tables to map PAR to the original PAN and all associated tokens.

4. Store a new EMV v2.0 data element (a "tag" that supports all EMV cards and terminals, as well as the Pay wallets and mobile apps) in the transaction message, although some card networks and their acquiring processors may not require this data element to be populated in the transaction message.

Many acquirers have not yet released their PAR specifications, leaving merchants unclear about the changes that are required to their systems or the complexity of integration. For larger merchants, any changes to the integration process are significant.

Other concerns relate to the practicality of PAR. Merchant relationships with a different acquirer and terminal provider create an extra step in the PAR process. The merchant must request PAR from its acquirer, which delivers it to the terminal provider in the authorization response. Adoption could be delayed by lack of coordination between the acquirer and the terminal provider. Acquirer systems cannot pass PAR to the merchant until they have made changes to enable the terminal provider to accept PAR.

Several merchants do not see PAR as a priority in the short-term. They may still be in the process of implementing EMV chip card technology or absorbing the investment in EMV chip migration. Some merchants may have already developed interim solutions. Others are waiting for direction from their acquirers and/or processors about how and when to integrate PAR.

Depending on the growth in Pay wallets and other tokenization use cases, it could be several years before broad adoption of PAR is achieved. Interestingly, some stakeholders suggest that PAR may eventually be issued for PANs in addition to tokens. Therefore, the PAR must be consistent across PANs whether they are lost, stolen, or newly issued to serve as an identifier that connects to a single account with all types of form factors.

With all this uncertainty, stakeholders need to determine their own strategies for PAR.

- Merchants need to ensure that their systems and those of their third party providers have the capability to carry PAR. While larger merchants may recognize the value of using PAR, smaller merchants likely do not when viewed in the context of the necessary resource investment and the lack of critical volume.

- Currently, issuers have little incentive to make changes to accept PAR, other than to be able to help a consumer if a merchant or acquirer cannot link a transaction to the PAN. The issuer's primary role is to manage the lifecycle of PAR to the PAN. Large issuers that maintain their own token vaults do not use PAR, but could accept it if necessary. If physical payment cards are tokenized in the future, then issuers will be involved.

- Processors do not have direct knowledge of what some merchants are doing or whether they have developed plans to integrate PAR; therefore, their primary focus is to ensure their applications can support PAR for second and third-tier merchants. Processors should also identify what services they can offer merchants to help them use PAR effectively.

- Card networks need to reach out to acquirers and merchants to better understand how merchants use PANs in their backend CRM or fraud modeling systems. They must also provide more education to stakeholders on how to leverage the PAR with tokenization.

- From a standards perspective, there are no required changes to ISO 8583 messaging to use PAR. The PCI SSC does not consider PAR to be PCI account data and on its own is not subject to the requirements for protecting PCI account data as specified in the PCI DSS.[39]

D. Internet of Things (IoT) and Wearables Applicability

In the next few years, industry experts believe IoT will have large scale implications for payments with a significant expansion in the number of devices that are capable of initiating remote payments, such as watches, automobiles, digital assistants, appliances, and more. Tokenization can be leveraged to secure the associated payment credentials stored on file to make payments from these connected devices. Domain restriction controls are also likely to play an important role in applying rules to establish limits on spending or the types of goods that can be purchased from disparate devices. Stakeholders that are evaluating IoT for payments want to understand the applicability of tokenization in a connected device environment.

The IoT industry is nascent and still under development, which leads many stakeholders to prefer a "wait and see" approach or undertake proof of concept tests to evaluate how to enable and secure IoT, and where to apply tokenization. It in unknown as to when IoT will achieve scale in the payments industry, but stakeholders find it necessary to plan for the future. Industry priorities remain focused on the mobile device and wallet, particularly since the majority of current IoT solutions share a connection to a mobile device.

Another complexity relates to the increased number of TRs in an IoT environment. Creating a unique token for every payment device is not a scalable solution with the delivery of the data. To address this, EMVCo introduced the concept of a *shared payment token* that enables a token associated with a particular PAN to be shared across multiple devices and secured with a cryptogram.

Stakeholder Perspectives

Merchant responses are mixed about the future of tokenization and IoT and vary depending on the type of merchant, goods offered, and the current status of their mobile payment strategy. Some merchants do not

[39] PCI SSC (2016, Jan.) *Is Payment Account Reference (PAR) as defined by EMVCo considered PCI Account Data?* FAQ response. Article Number 1374. Available at https://pcissc.secure.force.com/faq/articles/Frequently_Asked_Question/Is-Payment-Account-Reference-PAR-as-defined-by-EMVCo-considered-PCI-Account-Data.

see any applicability, based on their customer profiles or types of goods and services they sell. Others are monitoring developments to see if customer demand grows. Merchants recognize that the way customers shop will change and eventually they will shop through connected devices. As IoT becomes more prevalent, merchants may see customers adopt electronic payment methods in order to use IoT devices, since not all tenders are accepted electronically (e.g., cash, check).

Issuers and card networks are interested in the merchant IoT perspective to understand how they view all types of devices and what they consider important, particularly for security and interoperability with existing payment systems.

How payment data is stored in an IoT environment (e.g., in the device or the cloud) and whether the security is software or hardware-based is another key area of interest to stakeholders. Issuers need to know where to obtain the data they need to perform ID&V and ensure that the data is securely stored so that it can be used to validate the token and the customer.

The PCI SSC suggests the primary security focus should be to understand how and where tokens are generated, as well as the protection mechanisms provided by IoT solutions. IoT computational, storage, and power limitations, and potential for device firmware that cannot be updated, may limit the feasibility of secure approaches to tokenization for certain devices (e.g., calculating a token on the device may not be feasible). Provisioning of tokens and preventing misuse of a provisioned token may also pose security challenges. The PCI DSS is device-agnostic; therefore, the PCI *TSP Security Requirements (EMV Payment Tokens)* and *2016 Card Production and Provisioning Logical Security Requirements* version 2.0 can support a large array of IoT devices.

IV. Findings

1. **To Tokenize or Not Tokenize**. While use of payment tokenization will continue to increase, not all types of payments will need to be tokenized. For example, a digital prepaid card product that includes domain restrictions and dollar limits may not require a token. Larger merchants or payment service providers that apply security tokenization and have strong proprietary risk management systems may not deem payment tokenization necessary.

   Issuers decide whether or not to tokenize a particular type of payment card based on their own risk assessment.

2. **Consider Payments Tokens for e-Commerce**. Fraud risk in the e-commerce channel is growing as the number of transactions and associated dollar values continue to increase. Industry stakeholders must consider the benefits that payment tokenization can provide, particularly in an environment not supported by security tokens, such as CoF, recurring billing, browser-based transactions, IoT, wearables, and voice commerce. Stakeholders also want to ensure a convenient, secure, and frictionless purchase experience.

   Expanding payment tokenization into the e-commerce channel could benefit the industry in terms of reducing fraud by applying a consistent key security method across payment channels. Many merchants use security tokens to protect sensitive cardholder data; adding payment tokenization is a separate business decision. The industry needs to understand the benefits and challenges to using security and payment tokenization methods together to encourage merchants to consider payment tokenization.

Interoperable standards will play a pivotal role in driving ubiquitous security in e-commerce. The industry should monitor developments by EMVCo, ASC X9, W3C, and PCI SSC to ensure the development of interoperable, complementary, and flexible solutions.

3. **Third Party Token Service Providers**. Industry stakeholders support the expansion of third party TSPs and should evaluate and measure the benefits that they can bring to the payments ecosystem.

4. **Payment Account Reference (PAR) Number**. Stakeholder interest in PAR has been absent to date. A focus on education and awareness is needed to help stakeholders understand the value of using PAR, relevant use cases, and operational considerations. Smaller merchants may have limited knowledge about the value that PAR can bring to their operations and may benefit from more targeted communications between card networks, processors, and merchants.

5. **IoT and Wearables Technology**. The development and use of IoT devices will continue to grow and requires robust device security coupled with strong consumer authentication. The tokenization process for IoT is similar to that for mobile and digital payments, but requires further assessment of the methods needed to securely access and store data in an IoT environment. Stakeholders need to understand how the overall security and interoperability of IoT devices with existing payment systems will be ensured.

V. Future Considerations

Payment tokenization continues to demonstrate its value as an effective tool in protecting payment card data in the physical and electronic environment. However, its evolution is still nascent and subject to industry challenges as usage expands. As this growth continues, the industry should consider the following:

- How much consumer education for tokenization is needed? The expanded use of payment tokenization across use cases and channels will result in consumers having tokens in multiples places (e.g., CoF merchants, e-commerce websites, Pay/digital wallets, digital assistants, etc.). Stakeholders involved in token processing need to unify their approaches to educating consumers on how and where their payment credentials/tokens are stored and secured in the mobile/digital environment. For example, some FIs offer services through mobile banking platforms to help customers understand and monitor where tokens versus PANs are used.

- Discussions about the opportunities and challenges related to expansion of tokenization to other use cases, such as DDA/ACH and other verticals (e.g., SSNs, healthcare, etc.).

- Assess potential improvements to EMV v2.0, such as the more efficient use of data fields in the specification to allow stakeholders to better use additional data to make improved risk management decisions (e.g., token user or token assurance fields). Also, evaluate the benefits of tokenization and domain restriction controls for physical payment cards in the future, the potential impact to industry stakeholders, and how to prepare for this potential shift.

- Monitor and assess the interoperability considerations for the *EMV Secure Remote Commerce Technical Framework* (SRC Framework)[40] and payment tokenization.[41]

- Anticipate the ubiquitous adoption of tokenization by the industry and consider what the next innovative technology will be for securing mobile and digital payments. The industry should raise questions as to whether or not tokenization will be enough to secure the payments environment for the foreseeable future.

[40] EMVCo (2017, Oct.) *EMV Secure Remote Commerce Technical Framework Version 1.0.*

[41] For a discussion about the SRC Framework and industry considerations, see Pandy, S. and Crowe, M. (2018, August). *Securing mobile/digital payments in a global, transit, and faster environment.* https://bostonfedcm.ws.frb.org/publications/mobile-payments-industry-workgroup/securing-mobile-digital-payments-in-a-global-transit-and-faster-environment.aspx.