Is Payment Tokenization Ready for Primetime?

Perspectives from Industry Stakeholders on the Tokenization Landscape

Marianne Crowe and Susan Pandy, Federal Reserve Bank of Boston
David Lott, Federal Reserve Bank of Atlanta
Steve Mott, BetterBuyDesign

June 11, 2015

Marianne Crowe is Vice President and Susan Pandy is Director in the Payments Strategies Group at the Federal Reserve Bank of Boston. David Lott is a Payments Risk Expert in the Retail Payments Risk Forum at the Federal Reserve Bank of Atlanta. Steve Mott is the Principal of BetterBuyDesign. The views expressed in this paper are solely those of the authors and do not reflect official positions of the Federal Reserve Banks of Atlanta or 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

I. Executive Summary

The Mobile Payments Industry Workgroup (MPIW),[1] established in January 2010 by the Federal Reserve Banks of Boston and Atlanta, meets several times a year to share information and ideas, and discuss the barriers and opportunities resident in retail mobile payments, with a shared goal of building an efficient, secure and ubiquitous mobile payments environment in the U.S. Since 2010, the mobile payments environment has changed rapidly, adding new technology platforms, solutions, and participants to compete for consumer spend. Yet one long-standing barrier to achieving success has been the lack of a framework to secure the payment credentials and associated end-to-end mobile payment transactions.

Tokenization is one way the industry is embracing this security gap. In June 2014, the MPIW met with industry experts involved in tokenization from The Clearing House (TCH),[2] The Payment Card Industry Security Standards Council (PCI SSC),[3] and the American National Standards Institute (ANSI) Accredited Standards Committee X9 (X9)[4] to learn about the different tokenization schemes under development.[5] One outcome from the meeting was to form a sub-group to analyze the different tokenization schemes in more detail, with a focus on the *EMV Payment Tokenization Specification – Technical Framework v1.0* (EMV specification).[6] This analysis included a review of the structure and responsibilities of the card networks, card issuers,[7] issuer and acquiring processors, and merchants in the provisioning and processing of mobile and digital tokenized payment transactions under the various schemes; and discussion of Apple Pay as a use case.

This white paper will share what the group learned by providing an overview of the current U.S. payment tokenization landscape for mobile and digital commerce (vs. physical card payments); and describe how the different tokenization systems interoperate and the status of their implementation plans to a broader audience of industry stakeholders, policymakers, and regulators.

Success in implementing a secure framework using tokenization and other security tools will require extensive collaboration among participants to ensure that consumers have a cohesive solution. Moreover, it should be a solution based on agreed upon standards, rules, and practices that ensure seamless interoperability regardless of the mobile device, mobile operating system (OS), financial institution (FI), payment network, merchant, or wallet provider involved in the consumer's desired transaction.

---

[1] See http://www.bostonfed.org/bankinfo/payment-strategies/mpiw/index.htm.

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

[3] Launched in 2006, 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.

[4] 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.

[5] Federal Reserve Bank of Boston. (2014, September). *Summary of Mobile Payments Industry Workgroup (MPIW) Meeting Discussion on the U.S. Tokenization Landscape - June 2-3, 2014*. Available at http://www.bostonfed.org/bankinfo/payment-strategies/publications/2014/summary-of-mpiw-meeting-june-2014.pdf.

[6] EMVCo (2014, March). *EMV Payment Tokenization Specification – Technical Framework*. Available at http://www.emvco.com/specifications.aspx?id=263.

[7] Throughout this paper, the term, "card issuer" is used interchangeably with the terms "financial institution" and "issuer."

Generally, the foundation of a successful tokenization effort is one that is open to multiple business models; protects payment credentials and related transaction information; meets the needs of consumers and merchants for speed, ease of use and consistency; is standards-based; and supports long-term viability.

This paper represents the authors' views based on input from MPIW members and other stakeholders who were interviewed. It discusses benefits, challenges, gaps, and opportunities from the perspectives of the major industry stakeholder groups, while acknowledging that there is not necessarily full agreement on current approaches and/or underlying details that are laid out in the paper. By describing the current landscape and the related issues, our goal is to encourage further collaboration among the stakeholders to resolve differences to the mutual satisfaction of the industry and provide what is best for consumers.

II. Introduction

Until recently, tokenization in the payment space was primarily applied by merchants, acquirers, and technology providers in proprietary, closed environments post-authorization to protect data-at-rest. Tokenization eliminated card data from their systems and the payment risks associated with being hacked. As data breaches and other card-related compromises have increased, the need to utilize solutions that secure payments data from end-to-end has grown. This scope includes card-not-present (CNP) payment forms such as ecommerce and mobile payments.

To supplement the tokenization analysis undertaken by the MPIW subgroup, we conducted an industry stakeholder assessment, and interviewed 31 organizations, including card networks, large and small financial institutions, some which are card issuers, payment processors, online payment providers, merchant groups, mobile carriers, mobile wallet solution providers, and standards bodies. The organizations shared their views on the benefits and challenges of tokenization, if and how they applied tokenization in their businesses, and their familiarity and involvement in the EMVCo[8] and/or TCH payment tokenization initiatives.

The paper presents several major areas related to the evolution of the tokenization landscape as follows:

- An explanation of different types of tokens, including definitions of security and payment tokens, which replace sensitive card data with "tokens" that are unusable by fraudsters and have no value outside of a specific merchant or acceptance channel.

- An explanation of the relationship of tokenization to encryption, which involves encrypting card data so that it cannot be read and monetized by those attempting to commit fraud.

- An understanding of the major payment/card issuer and security tokenization initiatives, including TCH, PCI, X9, and a more detailed explanation of the EMV specification components.

[8] EMVCo LLC is a consortium that manages the EMV standard for chip and tokenization specifications. It is jointly owned by American Express, Discover, Visa, MasterCard, JCB, and Union Pay.

- An overview of the roles of card networks, processors, and online payment providers in tokenization, and how card issuers and merchants perceive the current tokenization landscape.

The paper concludes with key issues that need to be addressed and recommendations on next steps for the MPIW and the payments industry to secure the payment system and prevent payment fraud.

III. Overview of Tokenization

Since payment stakeholders use tokenization to address their specific needs, a number of different tokenization models have developed over the years. These models can generally be divided into two groups: *security tokens*[9] and *payment tokens*.[10] *Security tokens* (also referred to as post-authorization tokens) are used to replace the underlying sensitive value (e.g., the primary account number or PAN[11]) with a non-sensitive token value after the payment authorization process has begun or for data-at-rest (e.g., in a merchant database). Security token models for Point-of-Sale (POS) and ecommerce have existed since the mid-2000s, driven primarily by the issuance of the PCI SSC Data Security Standard (PCI-DSS) in 2004, which defines business requirements for protecting cardholder data.[12] The intent of the PCI SSC *2011 Tokenization Guidelines*[13] and proposed X9 requirements are to use tokens to secure and protect sensitive information (i.e., low value token), not to create a token to replace a payment credential used during a financial transaction (i.e., high value token) and processed over a payment network.[14]

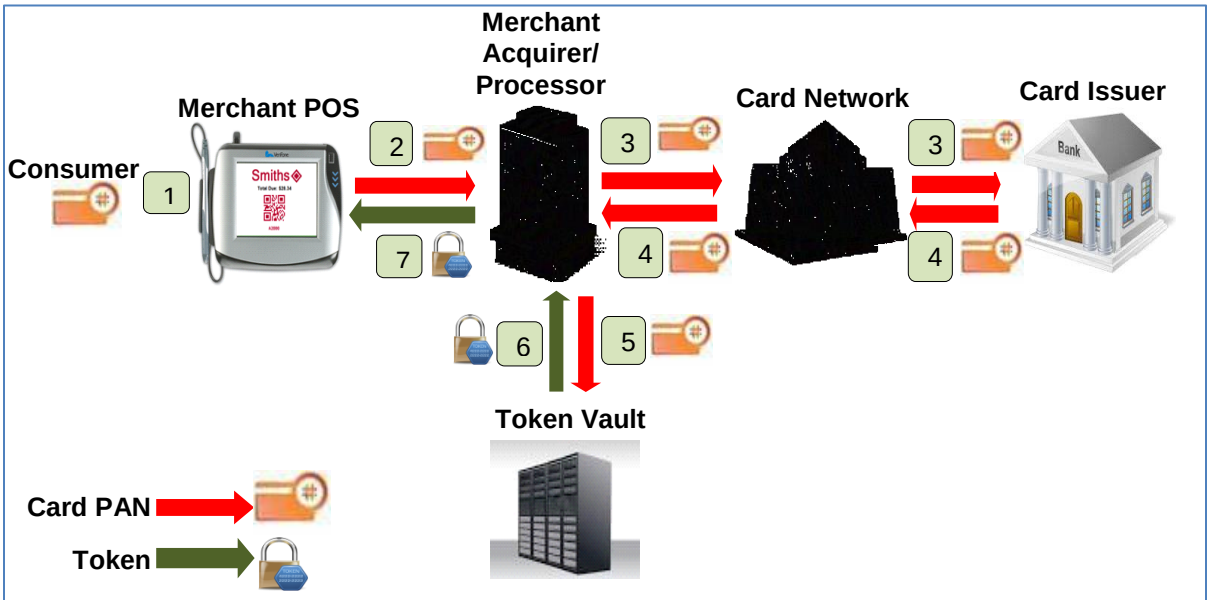
Historically, merchants stored PANs as reference points for back-end functions, including settlement, reconciliation, and authorization of card-on-file (CoF) transactions, chargebacks, identifying cardholder transactions for loyalty programs, and customer service. However, with a security tokenization model merchants can replace PANs with tokens in their archives to decrease fraud exposure and some of their PCI-DSS compliance burden.

Figure 1 describes the security tokenization flow. A customer swipes her payment card at the POS terminal which reads the magnetic stripe data (1). The POS terminal encrypts[15] the card track data (including the PAN) and sends the data to the Merchant Acquirer/Processor (Processor) (2). The Processor sends the transaction data to the Card Network which passes the data to the Card Issuer for

[9] We recognize that there are many definitions of security tokens in the industry and this paper is not referring to hardware-based security tokens that may be used for authentication (i.e., key fob or smart card) that allow the owner to authorize access to a network service.
[10] 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.
[11] The Primary Account Number or PAN is a number embossed on the plastic credit or debit card and encoded on the card's magstripe. It identifies the card issuer and the cardholder account. The number is 16 digits and includes a check digit as part of the authentication.
[12] Available at https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf/.
[13] Payment Card Industry Security Standards Council. (2011, August). *Information Supplement: PCI DSS Tokenization Guidelines.*
[14] Per the PCI SSC *2011 Tokenization Guidelines*, a low value token is a security token and a high value token is a token used in lieu of cardholder data to perform a transaction. PCI SSC considers high value tokens to be payment instruments.
[15] To avoid passing the PAN in the clear and leaving it exposed between the POS terminal and the acquirer, the transaction should be encrypted immediately at the time of card swipe and transmitted over a secure connection to the POS terminal.

the authorization decision (3). The Card Issuer returns the authorization decision back through the Card Network to the Processor (4). The Processor then sends the transaction data to the Token Vault to be tokenized (5). The tokenized data is sent from the Token Vault back to the Processor. The Processor matches transactions to the token data and stores the token in place of the PAN (6). The Processor sends the authorization decision with the tokenized data to the POS terminal. The POS system retains the token (but not the PAN) and the transaction data for its records (7). The Processor stores the static token and associated PAN in its Token Vault, to be used for recurring transactions and other PAN-related tasks that occur after authorization, including settlement, reporting, reconciliation, and chargebacks.

Figure 1. Security Tokenization Flow



Source: Federal Reserve Banks of Boston and Atlanta

Payment token models that replace PANs are a more recent development of the card networks and supported by the release of the EMV specification in March 2014. Under the EMV framework for payment tokenization, Token Service Providers (TSP)[16] issue payment tokens to Token Requestors (TRs) on behalf of FIs. The payment tokens replace PANs and are provisioned and stored in the customer's mobile wallet prior to initiating a mobile or digital payment transaction.

A. Payment Token

A payment token is a random value that replaces a cardholder's PAN when initiating a payment transaction. In the EMV specification, the TSP maps the token to the PAN to provide additional security. The token is presented to a merchant for payment and maps back to the PAN stored in the TSP's token vault to obtain authorization to complete the transaction. Since the merchant

[16] The EMV specification defines a Token Service Provider as an entity that provides a token service comprised of the token vault and related processing. The TSP has the ability to set aside licensed BINs as Token BINs to issue payment tokens for PANs that are submitted according to the specification, p. 19. The TSP role is discussed further in Section V-A.

does not have the cardholder's PAN, if the transaction records were compromised a fraudster would only obtain the token value. The token value would be useless for future transactions because it is combined with a dynamic cryptogram.[17] The inability of the fraudster to obtain usable PAN data is the key difference between security and payment tokens.

Payment tokens can be dynamic, static, or a combination of both.[18] True *dynamic tokens* are valid either for a single transaction or for a limited number of transactions within a very short duration.[19] By the time a fraudster intercepts a dynamic token it has already expired and has no value. However, dynamic tokens require a new value to be generated for each transaction, which creates challenges for the card networks, merchants, and processors. Dynamic tokens limit the ability to consolidate individual cardholder transactions, operate loyalty and marketing programs, and use transaction risk management applications. Management of dynamic tokens by the TSPs would also be more complex.

Because the value of a *static token* does not change, it can be multi-use, allowing merchants greater ability to connect the cardholder with transaction history. The EMV specification combines a static token with a dynamic component (the uniquely generated cryptogram) for additional security. The FIs that were interviewed prefer static tokens with cryptograms as more logical and less costly to implement than dynamic tokens, and support the EMV specification. *Section IV–Payment Tokenization Schemes* provides more detail on tokens.

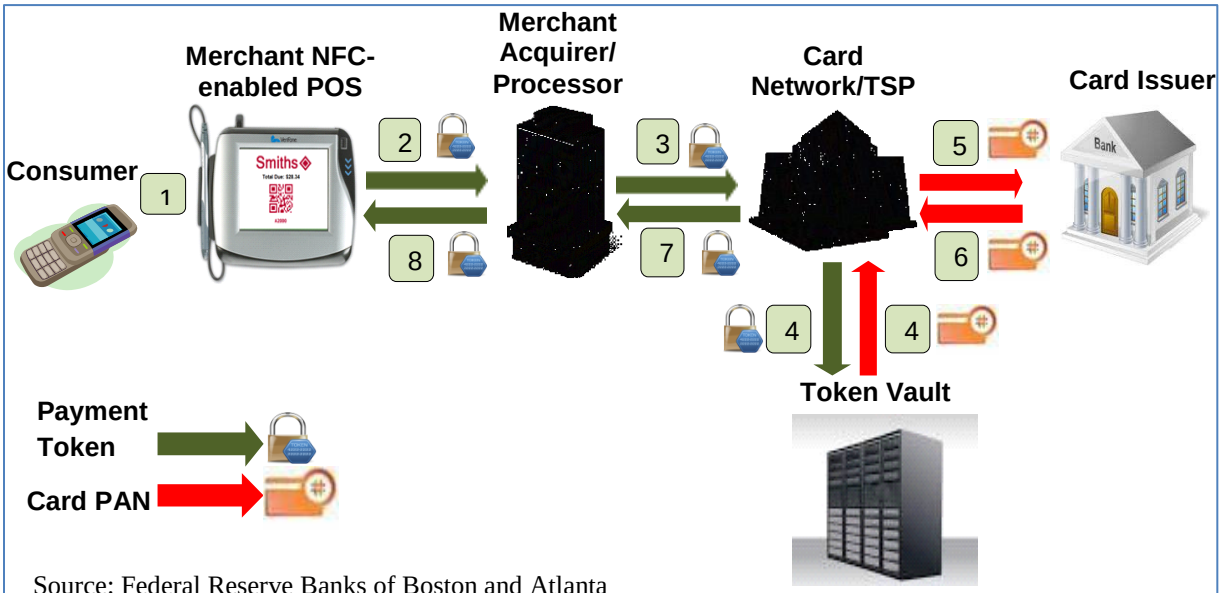
The EMV specification supports a static token with cryptogram model for several reasons: (1) it is difficult for some card issuers to deploy dynamic tokens to the key management configurations in their authorization/authentication systems; (2) at some point the networks could run out of available Bank Identification Numbers (BINs) to assign to all the different types of devices, domains, and use cases if they were dynamic; and (3) merchants cannot easily link payment credentials to customers and determine fraudulent transactions using dynamic tokens. Maintaining a static BIN as part of the token also follows the network routing logic and lessens the development effort required by various stakeholders to support such a tokenization scheme. Overall FIs understood the benefits of re-using tokens (static) versus discarding a token after each use (dynamic).

Figure 2 describes the payment tokenization flow per the EMVCo tokenization framework. To make a purchase at the merchant POS terminal, the customer uses his mobile device, which has been preloaded with a payment token stored in the secure element. The customer uses a fingerprint or passcode on his mobile device to authenticate himself and authorize the transaction to the terminal and verify the purchase amount (1). The POS terminal transmits the payment token, cryptogram and encrypted transaction data to the Merchant Acquirer/Processor (Processor) (2). The Processor sends the payment token, cryptogram and encrypted transaction data to the associated Card Network/TSP. The Card Network accesses the Token Vault to map the token and de-tokenize the PAN. The Card Network then sends the PAN from the Token Vault to the Card Issuer for authorization (5). The Card

[17] A cryptogram is a transaction security key that supports dynamic authentication or the use of changing variables unique to each individual card transaction. For a mobile transaction, the NFC chip generates the cryptogram in the mobile phone versus a chip on a credit card.
[18] While there are many other "types" of tokens, this paper will focus on static versus dynamic.
[19] True dynamic tokens are not widely supported and are explained here for background only. They are not addressed further in this paper.

Issuer returns its authorization decision to the Card Network (7). The Card Network then transmits the payment token and authorization decision back to the Processor (7). The Processor sends the authorization decision to the POS Terminal to complete the transaction (8).

Figure 2. Payment Tokenization Flow



Source: Federal Reserve Banks of Boston and Atlanta

B. Tokenization and Encryption

Tokenization and encryption are different types of data protection techniques. As discussed earlier, payment tokenization methods replace the cardholder credentials or PAN with a random set of characters that follow the PAN format, but that otherwise have no mathematical relationship to the PAN. Payment tokens cannot be reverse-engineered to find the related PAN. The PAN is not transmitted with the token, and only the token owner (i.e., TSP) has the key to map the token back to the PAN.

Encryption uses a specific algorithm derived from the payment credentials to encode the PAN and other data by masking the characters. The PAN is maintained, but requires authorized parties to use a key to decrypt or reverse the masked credentials back to the PAN. Without a decryption key the stored data is useless.

Security tokenization is effective if the PAN is not tokenized when payment is initiated. Even then, security tokenization only protects the PAN post-authorization and at-rest after the transaction process is completed. If the PAN is replaced initially with a payment token, the PAN is eliminated from the transaction flow, and some would argue that this eliminates the need for a security token to be created at all. However, until payment tokenization is ubiquitous, using a multi-layered combination of payment and security tokens, coupled with encryption, will increase the security of payment data. Fundamentally, this is viewed as the best available approach to payment data security for card, digital, and mobile payments (where tokens enhance the security of the near field communication (NFC) chip). Implementing only one solution leaves aspects of the payment system still vulnerable.

IV. Payment Tokenization Schemes

Financial institutions have been using tokens or pseudo-tokens in payments for initiatives such as the Universal Payment Identification System (UPIC)[20] and clearXchange[21] for some time. Merchant acquirers have offered security tokens for card-based payments to secure merchant systems for years. Yet the advent of payment tokenization is fairly recent, and incredibly quick to market. Due in a large part to this speed from concept to reality, TCH and EMVCo wrote and released similar token specifications during a one-year period. Given the desire of card issuers to see ubiquitous token acceptance, these similar specifications are aligning towards an interoperable token framework. The following sections provide more background on how the TCH (issuer-centric) and EMVCo (network-centric) payment tokenization schemes evolved.

A. Issuer Security for Card-Based Payments

In 2012, card issuing FIs began convening experts to discuss providing higher order safety and security measures for emerging mobile payments based on several motivating factors. First, EMV chip migration was becoming inevitable. One unintended consequence of better securing card-present (CP) transactions was that it made CNP transactions more vulnerable to attack in other countries. With mobile payments starting to gain traction, card issuing FIs also wanted to protect this nascent payment form factor (as well as existing CNP forms) before widespread adoption was achieved. Second, payment card data was increasingly under attack and some of these attacks were at entities out of FI control (e.g., merchants or other third parties). There was a desire to assist the entire ecosystem by removing sensitive payment card data from end-to-end.

In late 2012, large card issuing FIs and TCH began work on a standard for tokenization based on six guiding principles:

- **Open** – allows for different business models and fosters innovation
- **Safe and secure** – protects confidential personal, financial, and transaction information
- **Responsive to end-user and merchant needs** – Provides for ease of use, speed, availability, security, transparency, and consistency for users
- **Standards-based** – Establishes clearly defined standards which align with regulatory environment and avoids overlap with existing standards
- **Sustainable** – creates a path forward to support long-term viability and adapts over time as technology evolves; allows for an economically viable business model
- **Initial focus on high-risk use cases** – mobile and ecommerce, supports lifecycle management and exception flows, supports multiple form factors (e.g., NFC, QR codes); extensible to ACH

[20] A UPIC® is a unique account identifier issued by financial institutions that allows organizations to receive electronic payments without divulging confidential banking information. For more information, see https://www.theclearinghouse.org/payments/ach/risk-management/universal-payment-identification-code-upic.

[21] clearXchange is the first network in the U.S. created by banks that lets customers send and receive person-to-person (P2P) payments easily and securely using an email address or mobile number. For more information, see https://www.clearxchange.com/payments/.

The TCH effort resulted in a technical token specification in July 2013,[22] and a successful pilot in Q4 2013 involving live customer mobile payment transactions with card issuer, acquirer, and merchant participants. This original specification was shared with major card networks and relied on acquirers to identify tokens and route them to the token vault of record where de-tokenization would occur. Once de-tokenized, the acquirer would then forward the transaction to the payment network under normal authorization flows.

B. EMV Payment Tokenization Framework

For some time the major card networks have wanted to establish global standards to secure digital payments. They expected that the use of mobile platforms would grow exponentially over the next few years, creating new experiences for consumers, and raising concerns about increases in payment card fraud. The card networks identified challenges around the *proliferation of data* (credentials being passed and stored in multiple locations rather than the traditional ecosystem) and the *obfuscation of data* (what a card network sees is different from what the consumer presents to the merchant). As a result, they looked for ways to remove the payment card data from the transaction to reduce potential risks to the payments infrastructure.

The goal of the card networks was to develop a broad, common global standard to simplify the process for merchants to offer POS contactless, online, and other digital transactions that would complement the existing ecosystem and infrastructure and be managed through a standards organization. To support this goal, in October 2013, Visa, MasterCard (MC), and American Express (AmEx) announced[23] a collaboration using the existing structure of EMVCo as their defined standards body for networks participating to create their own token specification. The resulting EMV specification was released in March 2014.

Both TCH and EMVCo token frameworks relied on format preserving tokens to reduce infrastructure burden and increase adoption. While there were many similarities, there were two major differences. First, EMVCo defined a static token with dynamic components (cryptogram); whereas TCH defined a dynamic token. Second, and perhaps more importantly to the ecosystem, EMVCo established network-level awareness for tokens and enabled a de-tokenization flow between the network and token vault. Given the degree of alignment and FI commitment to a single industry standard, TCH agreed to align its effort to the EMVCo framework and sought membership in the EMVCo organization.

The fundamental purpose of the EMV specification is to enable universal use of tokens similar to the use of PANs. The specification espouses several principles: (1) ensure broad-based acceptance of a token as a replacement for the traditional card account; (2) enable all participants in the existing ecosystem to route and pass through the payment token; (3) enable digital wallet operators, mobile

[22] The Clearing House (2013, July 1). *America's leading financial institutions to collaborate on the safety and soundness of digital payments* [Press Release]. Available at https://www.theclearinghouse.org/press-room/in-the-news/2013/07/collaboration-secure-digital-payments.

[23] Visa (2013, October 1). *MasterCard, Visa and American Express propose new global standard to make online and mobile shopping simpler and safer*. [Press Release]. Available at http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1860500.

application developers, and others to easily and securely develop innovative payment products; and (4) improve cardholder security with tokens that are limited for use in specific environments.[24]

The EMV specification describes the payment tokenization ecosystem, the types of entities needed to support payment tokens, and key responsibilities of each entity within the ecosystem, along with the benefits of adopting a unified approach.[25] It also outlines minimum requirements for the creation and use of payments tokens, such as (1) token format similar to a payment card number: 13-19 digit numeric value that must pass basic validation rules of an account number in an International Organization for Standards (ISO)[26] message; (2) payment tokens must not have the same value or conflict with the PAN;[27] (3) tokens are domain specific, and only relevant within a specific domain; (4) for most use cases, the PAN is only known to the payment card issuer and customer, while the token is shared between merchants, payment processors, the customer, and other relevant parties to the transaction; (5) validating the identity of the Token Requestor (TR) each time a token is requested; and (6) type of token generated varies based on risk analysis–higher risk factors mean a low-assurance token. Token assurance and identification and verification (ID&V)[28] are discussed in further detail in *Section V–EMV Payment Tokenization Specification Structure and Process*.

The EMV specification will need to maintain compatibility with the existing payments infrastructure and complement existing specifications to ensure consistency across all payments environments as it is intended to be used by all payment networks and other payment participants.

C. Reaching an Interoperable Framework

Since the March 2014 release of the EMV specification, TCH was admitted as a business and technical associate in EMVCo, a class of membership allowing input to standards in progress. TCH participated in a number of EMVCo tokenization working group sessions and provided input and suggestions for enhancement of the EMV specification. As of June 2015, this work remains ongoing.

The EMVCo specification development process differs from accredited standards bodies, where membership is open and participants have voting rights. EMVCo solicits feedback through meetings with its associate members and their customers to evaluate and prioritize enhancements to future revisions. One change being considered is how to reduce industry stakeholder dependency on

---

[24] Boden, Rian. (2014, March 3). New EMV framework to support all types of mobile payment technologies, *The Mobile Wallet Report*, pp. 32-4. Retrieved from https://members.nfcworld.com/349/mobile-wallet-report-3-march-2014/ (Subscription required).

[25] The EMV tokenization specification complements the existing EMV Chip+PIN specification to ensure consistency across all payment environments and encourage global interoperability. EMVCo has engaged other industry partners to advance the specification and ensure cross-industry interoperability (e.g., through associate members).

[26] The International Organization for Standardization (ISO) is an independent, non-governmental membership organization and the world's largest developer of voluntary International Standards. It is comprised of 163 member countries that are the national standards bodies around the world, with a Central Secretariat that is based in Geneva, Switzerland. For more information, see http://www.iso.org/iso/home/about.htm.

[27] Networks must ensure that activities remain compatible to ISO specifications. Stakeholders must modify their payment business functions with the new method of presenting payment credentials.

[28] ID&V is a method through which an entity can validate the cardholder and the cardholder's account (PAN) to establish a confidence level for the payment token to PAN/cardholder binding. Examples of ID&V methods include: account verification message; risk score based on assessment of the PAN; use of one-time password by the card issuer or its agent to verify the cardholder.

the need for the PAN, while still making it possible for acquirers and others to perform tasks they typically do with the PAN.

The next version of the EMV specification should provide more clarity around the certification requirements for how third party processors and other entities can become TSPs and details on the TR registration process. Furthermore, a new identifier, the Payment Account Reference (PAR), is expected to be added to identify a PAN across multiple TRs and help merchants and acquirers reference back to the original PAN. EMV anticipates that its next version of the specification will be ready in the second half of 2015 or early 2016, and will share its proposed changes with members and associates when they are finalized.

Creating an industry standards framework for payment tokenization will simplify adoption for all participants and enable card networks to deliver the security and convenience that the industry needs to transition successfully to digital payments. A standard provides consistent methods to identify and verify a user before issuing a token, and commonality to simplify POS contactless and online transaction processing for merchants. As EMV chip[29] functionality is implemented in the U.S. to reduce counterfeit fraud for POS card transactions, the risk of fraud shifting to the mobile and online channels exists, so there is a strong desire by networks and card issuers to create tokenization standards to secure both.

D. Financial Institution Perspectives on EMVCo/TCH Tokenization Schemes

While several of the large FIs had participated in the original TCH pilot, all FIs interviewed indicated their support for the EMV specification. Card issuers would like the EMV specification to include more details on lifecycle management because these services vary by card network (serving as the TSP). The lifecycle management process allows the TSP to manage changes to the token and the PAN across different parties. For example, if a mobile device is lost, the TSP can generate a new token and provision it to the mobile phone on behalf of the card issuer. TSPs also can instantly replace a token linked to a PAN without reissuing a physical plastic card, which can reduce operational costs. Card issuers manage activities such as token expiration dates, token deletions, etc. The card networks have internet portals for card issuers to access the lifecycle management tools. However, card networks use the EMV specification as a guideline and may have unique implementations, (which is generally true for any standard), so card issuers need to code to a different Application Programming Interface (API) for each network.

Most FIs agree that the key criteria for any standard are ubiquity and scalability coupled with a good consumer experience. They view the EMV specification as an implementable reality that can achieve scale without any card issuer infrastructure changes, although they may need to work with TSPs to modify their enrollment verification processes and domain restriction controls. The EMV specification offers FIs more certainty on requirements, process flow knowledge, and a better indication of the success factors to support implementation and ongoing operation.

[29] EMV Chip is a global standard for card network participants.

E. Processor Perspectives on EMV Tokenization Specification

The processors interviewed represent acquirers, merchants, vendors, and gateways. Some believe that EMVCo is making more of an effort to engage the industry in response to initial dissatisfaction with the EMV specification. EMVCo has expanded its board of advisors and opened working sessions to solicit more feedback from the industry. About half of the processors interviewed formally participate as associate members of the EMVCo tokenization work group and a few others plan to join in 2015. A few processors believe that EMVCo restricts participation in the development of the EMV specification, and note that EMVCo's approach lacks an "open market" choice for merchants. The more optimistic processors think that EMVCo will be responsive in the long-term and engage processors to increase merchant adoption of tokenization. They all agree that technology solutions are best driven in an open environment, but recognize that developing open standards can slow down implementation. Therefore, processors would like to see EMVCo achieve a balance between inclusiveness and speed to market.

Processors feel strongly that they can help identify and develop functionality or features that would be useful to the market if given the opportunity to provide input on the how the EMV specification impacts merchant systems. For example, because tokens may represent different values for multiple parties linked to the same PAN, this may change how data analytics[30] are developed, reduce the benefit of velocity, impair the use of hot lists because they cannot map to the tokens,[31] and possibly require changes to customer relationship management (CRM) systems. The processors have discussed such merchant challenges with the card networks, who recently announced that they are exploring the development of a customer identification number, which, along with other benefits, will allow merchants and processors to link a cardholder with multiple tokens.

As noted earlier, processors have long supported security or merchant-centric tokenization schemes. They want to ensure that payment tokenization security controls do not disrupt merchant operations or systems, which could negatively impact merchant adoption. For example, format-preserving security tools do not disrupt merchant systems because they follow the PAN format.

Processors have differing views on the use of static or dynamic tokens. One processor noted that some components of the token need to be static to allow merchants to link multiple transactions to the same PAN. For example, maintaining a BIN as part of the token provides merchants with some visibility into the card network data. However, to prevent reuse outside of the authorized environment static tokens require external compensating controls. EMVCo combines the static token with a dynamic cryptogram to minimize this risk, which secures transactions and limits where or how the token can be used. If EMVCo promoted dynamic tokens instead, the industry would have to consider how to ensure enough capacity to support many more BIN numbers. One option would be to increase the size of the PAN and corresponding token from 16 to 19 digits, but processors raised concerns about the high level of system modification required to increase the number of digits to support a dynamic token.

[30] EMVCo is looking to address how to solve some of the operational and analytical challenges introduced with tokens.
[31] A hot list is a list of credit cards that are reported stolen, canceled or compromised in some way.

Processors also noted some merchant confusion about how an EMVCo payment token will synchronize with an existing merchant (security) token. This could be particularly confusing for small merchants when they consider products and services for their POS systems. The synchronization is referred to as "tokenizing a token," where the acquirer's processor is essentially handling an alternative PAN. The processors believe that a layered approach to payment and merchant-centric tokens could work as long as EMVCo does not make changes that interfere with the existing operation.

F. PCI and X9 Security Tokenization Models

The PCI SSC and X9 have separate efforts underway to develop security tokenization guidelines and standards, respectively. In August 2011, PCI SSC released *Information Supplement: PCI DSS Tokenization Guidelines* and in April 2015 it released *Tokenization Product Security Guidelines* for vendors and solution providers to use to develop tokenization products that help acquirers and merchants reduce storage of card data in their systems. The guidelines provide technical best practices that address the overall development of tokenization solutions, including: generation of tokens, how tokens are stored and retained for use (e.g., in back office systems), and implementation of products to address potential attack vectors and mitigate associated risks.

Security tokenization solutions must comply with PCI DSS to certify secure processing of PANs. PCI's premise is that if security tokens can be compromised and used to decode associated PANs, then it defeats the purpose of tokenization. Therefore, these tokens are within the scope of the PCI DSS and must be secured properly by ensuring that they cannot be reverse-engineered to reveal PANs. PCI also recommends that PANs and tokens not be stored together, except in the token vault.

X9, a fully open and accredited standards body,[32] is responsible for developing ANSI standards for the financial services industry. X9 is currently working on a two-part standard for encryption and tokenization. Like PCI DSS, X9.119-2 defines requirements for the secure implementation of tokenization for non-payment (security) tokens. It focuses on identifying how to secure a tokenization system and defining controls to prevent potential attacks against it.[33] Although it is not tasked to address the security issues around payment tokenization, by default X9.119-2 will provide useful guidance to companies building secure payment tokenization systems (e.g., more detailed guidance on specific mechanisms to implement PAN-to-token mapping). While X9.119-2 and PCI both address security tokens, X9.119-2 has a broader focus, aimed at building a standard around existing tokenization implementations.

[32] For more information on how to join X9, see http://x9.org/join-x9/membership-application/. For more information on how to join PCI SSC, see https://www.pcisecuritystandards.org/get_involved/join.php.

[33] This work is taking place in the X9F6 group that works on "Cardholder Authentication and ICCs (Integrated Chip Cards)." X9.119-2 defines tokenization as "the act of generating and mapping a token to an underlying sensitive value (USV)."

V. EMV Payment Tokenization Specification Structure and Process

A. Role of Token Service Provider (TSP)

The TSP is a combination of processor, personalization (perso) bureau, and trusted service manager (TSM)[34] and operates on behalf of the card issuer. The EMV specification covers TSP responsibilities at a very high level, including operation of a token vault to store and track tokens and their corresponding PANs. TSPs perform the generation, issuance, and provisioning of payment tokens for TRs (e.g., card-on-file (CoF) merchants, acquirers, processors, payment gateways, and digital wallet providers), lifecycle management, security and controls, TR registration, token assurance, and identification of token domain restriction controls. When transaction authorization is requested, the TSP maps the token to its PAN and either sends it directly to the card issuer for approval or to the processor serving on behalf of card-issuing clients.

Several payment industry participants, including alternative and debit networks, card issuers and issuing processors, acquirers, digital venues, and a few merchants, have expressed interest in becoming TSPs. Generally, industry stakeholders do not want or expect every organization to perform this function, since many do not have the necessary resources and expertise, but to provide a competitive market they want other qualified companies, in addition to the card networks, considered for the TSP role. Many large payment providers have strong security tokenization experience and currently perform TSP-like roles for their merchant clients. They could provide these services to other merchants, and/or card issuers, and assume that some of the large card issuers are also well-suited to be TSPs.

The current EMV specification provides no actionable detail on how to become a TSP, but at the same time it does not mention any restrictions. Currently, only card networks and a few large card issuers operate as TSPs. Large payment providers want more clarity and detail from EMVCo on the TSP requirements to determine eligibility, and would find it useful to understand the EMVCo requirements against an accredited industry standard. For instance, stakeholders raised several questions related to how a processor might remain competitive and manage multiple token specifications, how processors will integrate and interact with many TRs and still be able to provide a product that can work for everybody, how tokens will be integrated with the CoF model, and more clarity on network token pricing.

There are some benefits to having only the card networks fulfill the TSP role in the short-term. Because they develop proprietary standards, networks are able to react quickly to the market and modify specifications in step with market changes. Card networks have an advantage related to token deployment and management (TSP functions) driven by their expertise and experience related to the technological complexities of card provisioning and strong security. Card networks provide tokenization services and send issued tokens to TR processors (e.g., First Data or Fiserv), who provide payment services on behalf of their card issuing clients. They replace PANs with tokens that pass

[34] A TSM acts as a neutral broker in the NFC ecosystem by establishing business agreements and technical connections with mobile network operators, phone manufacturers or other entities controlling the secure element (SE) on mobile phones. The TSM enables service providers to distribute and manage their contactless payment applications remotely by allowing access to the SE in NFC-enabled mobile phones.

through the entire payment lifecycle as it is now structured for security.[35] Since both the merchant and card issuer need the token, for now it may be more efficient for the card network to create and link the token to the cardholder's PAN and pass the PAN to the card issuer as part of the transaction.

Because a TSP has the potential to hold millions of PANs and associated tokens in a token vault it must have extremely high levels of security to prevent data breaches, and reliability to ensure instantaneous accessibility from multiple channels. The provider holds all of the "keys" between the PAN and token value. Any criminal breach of the token vault would likely result in a major erosion of consumer confidence in the payments system since tokenization was intended to make the overall payment card system more secure. It is important that consumers trust the security of these companies.

Issuing processors are eager to assist their client FIs with implementation of Apple Pay but are limited to what they can do until requirements for becoming a TSP are released and they can determine if that is a role they want to perform. Until then, their client FIs must use the card networks as TSPs. Processors are concerned that once FIs are connected to a network TSP, it will be difficult to recapture that FI business due to conversion-related costs and changes, resulting in a potential loss of revenue.

B. Role of Token Requestor (TR)

The EMV specification provides a brief description of the role of Token Requestor (TR). A TR is an entity that procures payment tokens from a TSP to be used for completing a purchase. TRs include mobile wallet providers, shopping applications, web browsers, card issuers, merchants, acquirers, acquirer processors, payment gateways, and other payment enablers. A TR must register and comply with a TSP's proprietary requirements, systems, and processes. Once registered, the TR receives a Token Requestor ID and implements the specified Token API. The TR is then able to request tokens from the TSP to provision to customer NFC-enabled mobile devices containing secure elements for token storage.

C. Domain Restriction Controls

EMVCo believes that static tokens can be best protected by layering in multiple domain restriction controls. The EMV specification defines token domain restriction controls as "a set of parameters established as part of payment token issuance by the TSP that will allow for enforcing appropriate usage of the payment token in payment transactions. Some examples of the controls are: use of the payment token with particular presentment modes, such as contactless or ecommerce; use of the payment token at a particular merchant that can be uniquely identified; and verification of the presence of a token cryptogram that is unique to each transaction."[36]

TSPs are responsible for applying and executing domain restriction controls. During the registration process the TSP and TR work together to define and implement domain restriction controls that meet the TR's needs to protect payment tokens. For example, POS entry modes and merchant identifiers (e.g., such as country, region, different norms and markets, consumer demographics,

[35]The transmission between the card network and the card issuer (or the card issuer's processor) is a dedicated communication link that is constantly monitored for possible intrusion and the data is encrypted between the two entities. With this level of security practices, the potential to compromise the link and the data is low.

[36] *EMV Payment Tokenization Specification-Technical Framework v1.0,* p. 15.

customer profiles, levels of sophistication of customer base, loyalty, and average spend of consumer) are selected.[37] Domain restriction controls can also be created to limit token value, transaction volume or type of use (e.g., tokens can/cannot be used for digital goods), create expiration timeframes, set minimum token assurance levels, and add other elements. Using domain restriction controls to link a token to a specific TR prevents the use of that token at another merchant. Overall, domain restriction controls can significantly reduce the impact of fraud (albeit rare) from a compromised payment token.

Many industry participants outside of the network brands, including TCH and some card issuers, want more specificity and analysis on the potential impact of this component of the EMV specification. The EMVCo Tokenization work group's consideration of a variety of domain restriction controls is intended to help individual card issuers tailor their risk management preferences to token use, but more is needed to address concerns about possible inconsistencies related to consumer experiences. Further details on domain restriction control capabilities are expected in the next version of the EMV specification.

D. Token Assurance and Risk Scoring[38]

In addition to domain restriction controls, the TSPs assign risk scores or token assurance levels to tokens at provisioning. The token assurance level is a mechanism to identify the level of risk associated with a token, and is based on (1) the type and outcome of the ID&V process when the token is provisioned; (2) the entity that performed the ID&V; (3) the domain in which the payment token is to be used; and (4) supporting token assurance data.

The token assurance level can range from no assurance (00) to high assurance (99), depending on the strength of the ID&V methods applied and the TSP that confirms the results of the assessment. A token that is assigned a low assurance level faces several issues: (1) the token request may be declined; (2) the request may need an additional authentication method to be performed by the card issuer to ensure that the cardholder and his card credential can be verified; or (3) the TR may be charged a higher token fee.

Card issuers may factor in additional data fields to improve the level of confidence in the risk score or add information from their own authorization systems to authenticate the token. Token assurance levels are passed with each transaction, and optionally, the TSP's additional information can be included as part of the authorization request to the card issuer. Elements used to calculate the token assurance levels vary by card network or card issuer, and possibly by merchants in their roles as TRs.

EMVCo introduced the token assurance model to allow TRs to provide risk intelligence data about the transaction using the data that the card networks passed along with the transaction. The token assurance levels allow a card issuer to measure where the transaction may fall in their risk category. For example, solely using an address verification system (AVS) as an ID&V method may result in a low token risk score (01) and have policies associated with a specific network. A TR with CoF tokens could decide to increase the number of ID&V methods (e.g., device data, geo-location, IP address) to improve the token assurance level, which could improve fraud and risk assessments and

[37] An ID field identifies the merchant or other requestor that originally requested the token for the transaction.

[38] The EMV specification defines token assurance levels but does not provide requirements for implementation, although it is collecting input and will provide some guidelines in the future.

chargeback policy rights, depending on the card network which determines the policy rights for its scheme. Merchants have some control over the risk assurance score and can reject a transaction based on the assurance level.[39] They can also add more security features to generate higher (e.g., 99) assurance levels, but the trade-off may be customer convenience or privacy.[40]

One example of this trade-off involves sharing common tokens across merchants. Some merchant TRs may want to increase the token assurance value by implementing more authentication measures for their shoppers, which is how many ecommerce merchants operate today.[41] This becomes a servicing question as to whether the merchant wants to ask the customer for more details to reduce risk because it could lead to a negative customer experience and a higher customer abandonment rate. It is further complicated if the customer uses the same payment credential at another merchant and does not need to provide the additional authentication information.

Token assurance levels and ID&V are critical security underpinnings of the EMV specification. While the token represents an alternative value that reduces the exposure of the PAN in higher risk payment channels, including token assurance data can provide even greater security. Well-crafted assurance data can provide the necessary authenticity at a transaction level to allow a token to be re-used by generating cryptographically-derived unique data for each transaction.[42]

E. Identification and Verification (ID&V), Provisioning, and Authentication

The purpose of the ID&V process outlined in the EMV specification is to support secure and reliable payment transactions initiated with payment tokens. The token assurance and ID&V methods provide mechanisms and data to authenticate the cardholder of the payment token to a PAN and authorize use of that payment account. ID&V occurs as part of the token provisioning process. The card issuer examines the token domain restriction controls, risk assurance score, and any additional data to (1) decide whether to accept a token; (2) authorize the token for the transaction (e.g., matching device ID data if possible); and (3) handle exceptions (e.g., authorizing access to supporting data for returns, chargebacks, refunds, etc.). The TR may also provide data elements in the ID&V process that could be predictive of fraud, such as account age and history, bill to/ship addresses, IP address, device ID/information, geo-location, and transaction velocity. This data can be passed to the card issuer to aid in the authorization process. The ID&V process is discussed further in *Section VIII–Apple Pay*.

[39] The token assurance level is intended to establish transparency to the merchant and to drive common ID&V elements. Given an assurance level is returned in the authorization response, it would be impactful if merchants used the assurance level to reject the transaction.
[40] Personal interview with EMVCo Tokenization Working Group representative on September 29, 2014.
[41] Note that assurance levels do not change for each payment transaction authorization. A TR may request an increase to a token assurance value if it is implementing more authentication measures.
[42] Moser, Robin. (2014, July 2). *The real security with tokenization.* [Blog]. Retrieved from http://www.geobridge.net/uncategorized/the-real-security-with-tokenization.html.

VI. Network Role in Tokenization

Payment networks will use tokens universally in the same way PANs are used today. They add value by properly routing transactions and connecting millions of merchants and consumers globally in an interoperable way. Tokens are routable across payment networks and relevant in all places other than where the physical plastic card is used, including merchant CoF for ecommerce and device use cases, such as NFC.

Each card network has supplemental requirements that overlay the EMV specification. According to the card networks, some of the key elements of their specifications are: (1) new data fields to provide richer information about the transaction to improve fraud detection and expedite the approval process; (2) consistent methods to identify and verify a consumer before replacing the PAN with a token; and (3) a common standard designed to simplify the process for merchants to tokenize contactless, online, or other transactions.

A. Network Tokenization Challenges and Opportunities

There are several challenges and opportunities to a scalable network tokenization solution for payments. Challenges include limitations on available BINs, multiple users to one account/PAN, and data ownership. The opportunities lie in the potential for consistent, broad, and creative industry collaboration to increase payment security.

A token BIN (which identifies the issuing FI) is designated only for the purpose of issuing payment tokens. Payment tokens are generated within a designated token BIN range. A token BIN range is a unique identifier that consists of the leading 6-12 digits of the token BIN. Each card network assigns token BINs and BIN ranges to its respective card issuers directly and potentially to non-network TSPs in the future. The card networks include both token BINs and BIN ranges in the BIN routing table to support routing decisions by merchants and acquirers. The BIN ranges enable merchants and acquirers to choose preferred and cost-effective networks over which to route their tokenized transactions.

A card issuer may have more than one BIN, e.g., one for credit accounts and another for debit, and they can use ranges to classify credit, debit, and other products. The card networks maintain and publish token BIN routing tables, but managing and storing token BINs is a primary function of the TSP.

Stakeholders are concerned that current BIN range capacity is insufficient to support static (plus cryptogram) payment tokens. Card networks have begun to discuss how to resolve this issue. MasterCard plans address this challenge by maintaining the 16-digit BIN, but adding two more digits to the BIN range to increase it from 6 to 8 digits. They will distribute BIN ranges to card issuers instead of assigning wholesale BINs. MasterCard believes this will address the BIN shortage if everyone follows the same strategy. Using ranges will also reduce waste of dormant BINs.

Google has a different perspective on how to address the BIN issue. It is able to leverage a user's logged-in experience with Google across multiple devices to avoid creating a separate token for each device. Google can enable user level authentication regardless of device. Google supports

additional field length for tokens to accommodate more data, but in lieu of the token containing more data, it prefers to enable the message specification in its entirety to have room for additional variables.

In some cases, multiple users share one PAN or account. How to assign tokens to these joint account owners creates another challenge for payment tokenization. For example, a couple may have a joint account, but have payment cards for that account with separate PANs that are loaded onto their respective mobile phones. For each token request, a unique token is issued for Joe and a unique token for Mary, so the transactions associated with each token cannot be consolidated. Card networks address this issue in different ways. Some create a sub-account for each user of the shared PAN. Other networks attach unique sequence numbers and issue different tokens for the shared PAN. In this example, Joe and Mary each have a unique sequence number associated with their shared PAN. The token request identifies the PAN sequence number and includes it on either Joe's or Mary's specific mobile device to distinguish multiple tokens for the PAN. The EMV specification provides a Token Reference ID[43] (up to 99 values) to track multiple token values (e.g., different sequence numbers) that map to the PAN and track the individual who receives the token.[44]

The card networks (i.e., TSPs) have not gained any new ownership rights to tokenized data crossing their networks; however, they have gained access to debit network transaction volume, which they did not have with card-based (non-tokenized) transactions.

In March 2014, Visa and MC spearheaded the effort to form a new cross-industry group, the Payment Security Taskforce (PSTF), to focus on enhancing payment system security. Members of the PSTF are financial institutions, credit unions (CUs), acquirers, retailers, POS device manufacturers, and industry trade groups. The PSTF members want to enhance payment security by sharing ideas to break down barriers and spur adoption of next generation security solutions for the benefit of all. The group initially focused on the adoption of EMV chip technology in the U.S., but is also addressing related security topics, including tokenization and point-to-point encryption (P2PE). Based on its findings, the PSTF published a white paper discussing the *U.S. Payments Security Evolution and Strategic Roadmap* in December 2014.[45]

B. Network Tokenization Services

All four major card networks have either launched or are planning to launch tokenization services on behalf of card issuers, and may charge them fees for token vault services that provide for the generation and management of payment tokens, including mapping tokens to corresponding PANs.[46] As discussed earlier, some large FIs and processors also offer or plan to offer their own

[43] A Token Reference ID is a value used as a substitute for the payment token that does not expose information about the payment token or the PAN that the payment token replaces.
[44] The ISO version of the PAN Sequence Number (PSN), which defines different cards assigned to the same PAN, is also two bytes, so the EMV specification is in line with the current PSN standards.
[45] Available at http://usa.visa.com/newsroom/media-kits/assets/US-Payments-Security-Evolution-and-Strategic-Road-Map-for-Release.pdf.
[46] Both Visa and MasterCard released rate schedules for tokenization services in late 2014 but Visa has waived these fees until the end of 2015. For Visa, see http://www.pymnts.com/news/2014/visa-ceo-confirms-tokens-as-new-network-revenue-stream/ and MasterCard, see http://www.digitaltransactions.net/news/story/As-Card-Industry-Use-of-Tokens-Increases_-MasterCard-Plans-Digital-Enablement_-Fees.

tokenization services. The card network TSPs provide on behalf of services for Apple Pay, which is discussed in more detail in *Section VIII - Apple Pay*.

MasterCard Token Services

The MasterCard Digital Enablement System (MDES) is the MC token service, launched in September 2014 and currently used for Apple Pay. The MDES provides a unique device account number, or token, that is bound to the mobile device. This allows MC to control use of the token by the specific consumer and device authorized by a card issuer, including the ability to block illegitimate use of the token. After the token has been provisioned to a mobile device, each mobile transaction generates a secure one-time code, or cryptogram from the SE in the phone as part of the overall transaction message including the token value. The token is then remapped to the PAN seamlessly for authorization by the card issuer.

The MDES provides card issuers with lifecycle management functionalities to manage the creation of new and expiration of old tokens as needed. It also provides card issuers with APIs to build customer service tools that allow them to suspend or reactivate a token if the mobile device is lost or stolen. In the future, when MDES supports card-on-file (CoF), the same functionality will be available to those merchants to replace tokens, manage mapping by token vault, and perform cryptographic validation. Card-on-file merchants will also be able to perform customer service functions through an API.

Visa Token Services

Visa announced its Visa Token Service (VTS), which is part of the broader Visa Digital Solutions (VDS), in September 2014. VTS offers on behalf of services that enable FIs to process online and mobile device-initiated payments and supports token creation for all product types. Using VTS, Visa tokens can be stored in the mobile phone, in an ecommerce app, or in a cloud-delivered app. Tokens can be limited to use with specific merchants, devices, or categories of spending as controlled by the card issuer. The VTS service can instantly reissue tokens linked to lost or stolen mobile devices without changing PANs or reissuing plastic cards.

VTS provides Software Development Kits (SDKs) for merchants, FIs, and application developers to embed Visa PayWave contactless technology into mobile applications. Because Apple Pay uses it to invoke a Visa PayWave transaction to the merchant POS system, card issuers offering Apple Pay through Visa must support VTS. Card issuers can host account information in the cloud or on the SE chip in mobile phone. VTS is based on an ISO standard so it allows merchants, acquirers, and card issuers to process and route tokens similar to how they handle card payments and includes specifications for other mobile and digital platforms such as QR code, Visa Checkout, and NFC-enabled host card emulation (HCE).[47] It is also considering tokenization for non-Apple phones by working with those device manufacturers to implement VTS.

[47] Host Card Emulation makes it possible to perform NFC card emulation without using the secure element (SE) in mobile handsets. HCE enables NFC card emulation communications to be routed through the mobile phone's host processor versus from the POS terminal through the NFC controller to the SE.

American Express Token Services

American Express (AmEx) supports the EMVCo approach to obtaining broader adoption in an interoperable way and removing concern about payments fraud more naturally through payment tokenization. Prior to the EMVCo tokenization initiative, AmEx employed tokenization with other products that addressed the need to secure payments by eliminating the core data from the system and making the process transparent to all of the players in the value chain. The AmEx payment gateway provided security tokenization services to its merchants, together with other methods to protect the core data. The different tokenization methods (e.g., data-at-rest, localized acquirer, merchant level, and EMV chip) were done on a small, controlled level.

In November 2014, AmEx launched its payment token service in the U.S and plans to have the service available internationally in 2015 for AmEx brand card issuers and, presumably, for AmEx's own card issuing operation. The AmEx tokenization service designates domain restrictions (i.e., domain restriction controls) for use type which allows it to better control fraudulent transaction attempts. These domain restrictions also prevent skimmed tokens from being used at unauthorized ecommerce merchants by restricting the tokens to pre-determined CoF environments (i.e., ACME.com tokens can only be used within ACME.com).

In early versions of the contactless card, AmEx used an alias card number (a unique number in PAN format similar to a token) on the credit card to protect the security of the card number and prevent fraudsters from intercepting the real account number during transmission. Today, AmEx supports this form of payment tokenization via its Serve prepaid application, which can be accessed directly, and until recently through *Softcard*.[48] Serve assigns an alias to the customer's prepaid account, which is stored in the SE in the mobile phone. AmEx sets domain restrictions to prevent the Serve account from being used online.

Discover

Discover has been an active participant in the development of the EMV specification and announced participation in Apple Pay on April 27, 2015. Discover has stated in public documents that it plans to offer a tokenization service for its issuers in 2015. However, we did not interview Discover for this paper.

VII. Processor Tokenization Perspectives

Payment processors have been providing merchant-centric security token services for several years to address merchant data security needs. This section reflects the perspectives and experiences of several large payment processors, acquirers, and gateways (processors) on how they apply security tokenization methods. Payment processors use proprietary systems to perform security tokenization for merchants. They store the PANs post-authorization, but provide tokens to merchants to retain for their transaction records. While this process improves security to some degree, the PAN is still exposed prior to authorization and remains at risk unless the merchant is using point-to-point encryption from the POS terminal to the acquirer's processor.

[48] Google acquired Softcard in February 2015 and shut it down on March 31, 2015.

A. General Process

The payment processors interviewed have all developed proprietary security tokenization solutions for their merchant clients that generally operate in the same manner to help merchants eliminate the storage of card data and reduce the risk of a data breach, thus protecting them from financial and reputational harm. The security tokens substitute for PANs for data-in-transit and at-rest in a retail environment. One processor described its role in this process as "transferring risk from merchants to itself as it protects data in a way that is auditable."

B. How Processors Use Security Tokenization

One processor interviewed can support a token up to 32 alphanumeric characters, and can generate whatever type of token may be requested. Another processor uses a two-token system which generates a one-time use, low-value token over a secure channel. Merchants exchange it for a high value token that maintains the same PAN format. This processor assigns a different token to each merchant for the same cardholder PAN, so each token is unique to a specific environment, similar to domain restriction controls under the EMV specification.

One gateway processor described how it provides an ecommerce merchant-centric token solution for Apple Pay. The merchant uses the gateway processor's token for the customer ID. The Apple Pay token is a subset of that merchant-centric token solution. The gateway processor produces a token for the ecommerce merchant that can be mapped to specific payment transactions for that token.

VIII. Apple Pay

Apple Pay is a new iOS mobile wallet launched by Apple in October 2014 for iPhone 6 and 6 Plus phones, iPad Air 2, and iPhone 5 users paired with the recently released Apple Watch. Apple is unique among the mobile/digital wallet providers in that it owns and controls the mobile handset, mobile OS and the secure element (SE), and leverages iTunes[49] to source Apple Pay accounts and its Passbook application to integrate the accounts.

The new iPhones contain NFC chips and embedded SEs that allow users to tap and pay for purchases at NFC-enabled POS terminals, or use retailer mobile applications that offer the in-app version of Apple Pay. Users manually load payment cards into Apple Passbook or use the phone's camera to scan their credit and debit cards (no picture is taken or stored). Users can select their iTunes payment card to activate in Apple Pay. While Apple has access to payment credentials for accounts in iTunes, it does not have access to the underlying PANs on new cards loaded into Passbook, nor will it have access to the tokens stored on the embedded SE. The Touch ID fingerprint (or a passcode) uses an authentication protocol to validate the customer's identity at the POS checkout or in-app purchase to prove both the mobile device and the authorized cardholder are physically present in the store.

[49] Apple has approximately 800 million iTunes accounts.

A. Apple Pay Token Provisioning and Transaction Flow

Provisioning: When a user enrolls a payment card (PAN) into his iPhone, Apple contacts the TSP to request permission from the card issuing FI that owns the card to enable Apple Pay. The card issuer authenticates the cardholder's identity, which is a critical step in the provisioning process to prevent fraud. The card issuer will complete the ID&V process by approving the request without further verification (i.e., green path), or getting further verification by using out-of-band authentication (e.g., one-time passcode), or by directing the customer to the call center to guarantee that the customer is in good standing (yellow path). If approved, the card issuer transmits the PAN to the appropriate TSP[50] to generate a token.[51] The network sends a payment token to Apple's TSM to provision into the embedded SE on the mobile device.[52] Apple Pay PANs are never shared with or stored with Apple or in the mobile phone.

POS NFC Transaction Flow: To make a POS purchase using Apple Pay, the user holds his phone over the POS terminal. The mobile app in the NFC-enabled mobile phone will recognize Apple Pay and prompt the user to authorize the transaction with his fingerprint using Touch ID or with a passcode. The card used for payment is the user's default card in the Passbook app. After Touch ID verifies the user's identity, the payment token, cryptogram, and transaction data are transmitted via NFC from the embedded SE in the phone to the POS. The POS system forwards the request via the acquirer to the TSP. The TSP maps the token to the PAN stored in the token vault, inserts the PAN into the authorization request, and sends it to the card issuer. The card issuer receives the authorization request, approves or denies the transaction, and returns the decision back through the card network and acquirer to the merchant POS. When the transaction is complete, the phone beeps or vibrates and an on-screen "checkmark" and "done" notification is displayed. The customer will receive either a paper or email receipt, based on preference.

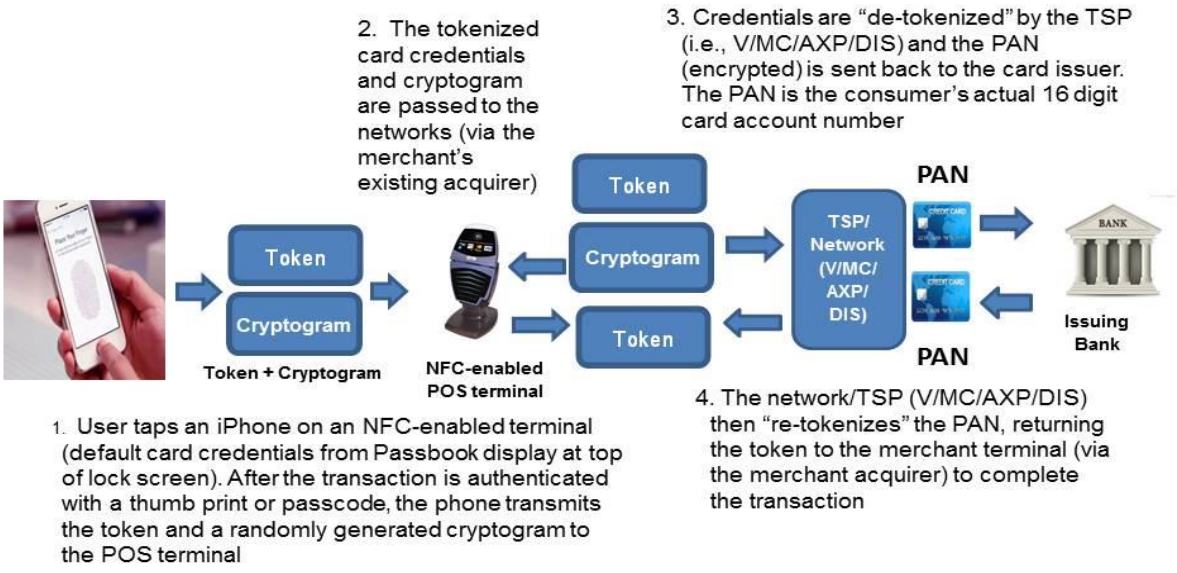
In-App Transaction Flow: Apple Pay offers an in-app solution which allows users to pay with a merchant's mobile app by displaying a "Pay with Apple" or "Apple Pay" button in the app. An electronic receipt is provided to the customer upon completing a transaction. When the user clicks the button, Apple Pay retrieves and processes the static token stored in the embedded SE on the iPhone, together with the dynamic cryptogram generated by the embedded SE, the token expiration date, transaction dollar value, and any additional data Apple passes.[53] The Apple Pay in-app dynamic cryptogram is different than the EMVCo cryptogram for contactless cards as this is considered a remote (ecommerce) transaction.[54] If merchants use 3-D Secure (3DS),[55] they will receive and pass the

[50] Apple is the Token Requester. Visa, MC, and AmEx, along with a few large FIs, currently serve as TSPs for Apple Pay.
[51] The PAN is converted to a randomized string of numbers and stored in a virtual token vault.
[52] It is bound to both the iPhone device ID and the customer's PAN. The SE in the iPhone generates a dynamic cryptogram (using EMV-type encrypted data) for each transaction. The token, combined with the card network's security process and Apple's TouchID thumbprint verification used by the customer to approve the transaction, is viewed by the networks as sufficiently secure to be assigned card-present interchange rates.
[53] For Apple's "in-app" option, the generation and receipt of the cryptogram is not completed as a full EMV/NFC transaction (which is the only transaction that warrants card-present rates in the bankcard world). Instead, the 3-D Secure key, also part of the payment token, is used to complete the 'in-app' transaction, and charged card-not-present premium rates, with the merchant bearing the liability, similar to other ecommerce transactions today.
[54] EMVCo would like Apple Pay to generate an EMV cryptogram, which consists of the encrypted CVV combined with some unique transaction data—as configured with EMV cards. But the CVV is not collected independently of the token information, so the Apple Pay cryptogram generated online is based on a 3DS key.

cryptogram in the 3DS field of the ecommerce transaction. 3-D Secure is discussed in further detail in *Section XII-Tokenization in Ecommerce*.

Several payment providers (e.g. Braintree, Stripe, Authorize.net, Chase, Cybersource, First Data, and TSYS) use SDKs to develop applications that support Apple Pay for their merchants.[56] Figure 3 illustrates the Apple Pay transaction flow.

Figure 3. Apple Pay Transaction Flow



Source: Federal Reserve Bank of Boston, compiled from various sources

B. Stakeholder Experience with Apple Pay

Financial Institution Experience - Identity and Verification (ID&V)

Apple Pay affords FIs the potential to collect more data about the enrollment process (e.g., information about the mobile device or the iTunes account)[57] to inform and enhance the ID&V or risk-decision process. Apple will provide iTunes information directly to some card issuers and through TSPs to others. For example, information might include: 1) whether the card account being enrolled is

[55] 3-D Secure (3DS) is a secure communication protocol used to enable real-time cardholder authentication directly from the card issuer during an online transaction to improve online transaction security and encourage the growth of ecommerce payments.

[56] For a current list of providers, see https://developer.apple.com/apple-pay/ or https://developer.apple.com/apple-pay/Getting-Started-with-Apple-Pay.pdf

[57] Some additional information can be included in the ISO 8583 message fields that the FI/issuers can review as part of their risk decisioning. For example, the cryptogram is authenticated, as well as the token and the wallet service provider that the token came from.

already in iTunes; 2) how long the account has been enrolled in iTunes; and 3) whether it has been used in the last six months. Media sources suggest that Apple provides the geo-location, the last four digits of the mobile phone number, device name, and iTunes activity for that card.[58] While FIs are unsure about the level of detail they will receive from Apple or how that data may be used for other purposes, they agree that the token opens a new world in terms of potential for helping to manage risk.

Each card issuer receives specifications and guidance from Apple to establish the ID&V process and token issuance. The card issuers work with their card networks (TSPs), or with their processor that interacts with the TSP on their behalf, to create the rules to review the Apple data. During the ID&V process, Apple passes data to the card issuer to match against its own data. If a customer fails authentication in the provisioning process, the card issuer will provide a portal and/or 800-number for the customer to call (see Yellow Path Authentication section below). Card issuers are still in the process of determining how to monitor all the data tied to the Apple Pay roll-out. Some card issuers have established supplemental ID&V processes and can request additional information to make decisions about activations. Because FIs want to make their own risk management decisions, many are eager to control as much relevant data as possible in-house. However, card issuers that cannot build their own ID&V infrastructure because of the investment must rely on the Apple Pay ID&V infrastructure or on their processors to provide this service.

The card networks' rules for setting up the Apple Pay ID&V process vary, which presents a challenge to card issuers, requiring them to build separate applications for each network they support. Also, each network stores the tokens and data elements that are part of the ID&V process in different fields in the ISO 8583 data message (i.e., each network interprets ISO 8583 differently). At the same time, card issuers are driving some of the business needs to enhance ID&V. For example, some card networks allow card issuers to use more of their own data in the enrollment/provisioning process.

Provisioning: Some card issuers expressed a preference to have their cardholders complete the provisioning process by logging into their mobile banking application. This would allow the FI to present knowledge-based authentication (KBA) and provide additional security around provisioning the account. After the provisioning process, the card issuer begins to develop intelligence on the card behavior so that it can evaluate when that behavior begins to indicate higher risk and trigger the need to monitor a transaction more closely.

Authentication: Card issuers are taking different approaches to the enrollment authentication process because they have varying risk tolerances. While most card issuers will make their own determination as to whether or not additional authentication is needed, the card networks provide tools to issuers to establish criteria that enable the card networks to authenticate a request on the issuer's behalf.

Yellow Path Authentication: When a new card is added to Apple Pay, the card issuer must verify that the individual loading the card is the actual cardholder to prevent an unauthorized user from adding someone's card to another phone. When this verification process requires additional

[58] Graham, Bob (2015, March 25) Commentary: Banks are responsible for weak authentication in Apple Pay fraud. *Digital Transactions*. Retrieved from http://www.digitaltransactions.net/news/story/COMMENTARY_-Banks-Are-Responsible-for-Weak-Authentication-in-Apple-Pay-Fraud.

investigation by the card issuer it is called *Yellow Path Authentication* (conversely, when a card is automatically accepted, it is considered "Green Path" and when it is rejected it is "Red Path"). Until a month before the official launch of Apple Pay, *Yellow Path* authentication was optional for card issuers. When it became mandated many card issuers had to quickly assemble support for card-user authentication, which resulted in different levels of rigor to improve *Yellow Path* authentication.

Some card issuers compare Apple Pay account details to their cardholder information and use a two-step authentication process by using out-of-band-authentication (OOBA), e.g., sending a validation request to the user's mobile phone number through a separate mobile application or via email, and others require users to contact a call center for additional verification. Some call centers have experienced problems if they are asking customers only simple KBAs (e.g., mother's maiden name, last four digits of their Social Security Number, etc.), since that information is relatively easy for fraudsters to obtain. These less effective approaches to Yellow Path authentication resulted in fraudulent cards provisioned into Apple Pay. According to First Annapolis, approximately half of the Apple Pay card registrations require additional authentication, so it is an important part of the onboarding process.[59]

Early Apple Pay card issuers expressed that they would have benefitted from more lead time to fully evaluate and improve the provisioning process before deployment. However, Apple wanted card issuers to get as many green path approvals as possible to encourage initial adoption and minimize customer friction. The less stringent provisioning processes led to higher levels of fraud from stolen card credentials used to create Apple Pay accounts, obtain fraudulent tokens, and use them to conduct fraudulent transactions. Responses from several large FIs after the news about increased fraud with Apple Pay were somewhat temperate. They indicated that since their initial program launch they have upgraded their enrollment authentication requirements and processes, resulting in significant decreases in their fraud rates. In March 2015, one large FI reported only 35 cases of fraud out of thousands of Apple Pay customers.[60] At the same time, this situation shows that some participants are still learning about the risks associated with a move to digital accounts and mobile wallets. As they identify best practices in this new payments area, they realize the need to take the time for proper due diligence, as with any new payment solution.

Best Practices for FI Enrollment Authentication with Apple Pay

It is the responsibility of the FI to authenticate the cardholder during the enrollment process. Based on the interviews conducted with several large and small FIs, the larger FIs appear to be better positioned to handle the challenges of Apple Pay provisioning. However, smaller FIs may need more assistance. Several best practices are outlined below:

1. Do not limit validation to static account data/PAN only as this data may have been compromised by a data breach.
2. Leverage other mobile authentication services (e.g., Payfone).[61]

[59] Brown, Ben. (2015, February). Apple Pay: Early observations on potential fraud exposure. *Navigator*. Published by First Annapolis. Retrieved from http://www.firstannapolis.com/articles/apple-pay-early-observations-on-potential-fraud-exposure.
[60] Sidel, Robin and Wakabayashi, D. (2015, March 5). Apple Pay stung by low-tech fraudsters, *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/apple-pay-stung-bylow-techfraudsters-1425603036?KEYWORDS=pnc+bank.
[61] Payfone is an example of a mobile authentication company working with U.S. FIs to utilize the same security standards applied by wireless operators to identify their customers as they log-in to mobile banking apps. Payfone's Identity Certainty

3. Monitor patterns in a customer's mobile account lifecycle.
4. Leverage channels beyond the call center to authenticate customers. For example, if the customer fails identification questions or locks his mobile banking app, then consider sending him to the physical branch or use out-of-band authentication methods.
5. Closely monitor spending activity across all channels on new digital accounts to identify fraud patterns and quickly suspend suspicious accounts.
6. Train call center staff to not "help" the caller guess at answers to security questions or passwords.

Financial Institution Experience – General

All of the large FIs that were interviewed are currently involved with and expressed strong support for Apple Pay as a consumer tokenization solution based on the underlying security, capacity for scalability, and comfort level with data management. Scalability of tokenization is possible because Apple Pay uses a card network-driven switch that follows the credit card BIN format. There is a general consensus among large FIs that mobile phone based transactions have a greater degree of security than other types of payment, particularly given the potential ability for the user to remotely wipe his phone if it is lost or stolen.

To date, FIs report positive experiences with the Apple Pay rollout as well as good user experiences, but recognize that these results are preliminary. FIs are relatively satisfied with the transaction process because of Apple Pay's unique infrastructure for authentication and authorization. Their main concerns are the provisioning process and the potential for in-app purchases to expose a new fraud channel.

For most FIs, testing to support Apple Pay has involved complex work, mostly because many have card systems not designed to handle the complex one-to-many token-to-PAN relationships. One card issuer explained the extensive infrastructure changes that were required to support real-time account provisioning and customer authentication in order to put their credentials somewhere else, e.g., to take the token request and use it later as a payment vehicle. Overall, FIs like the way the process is designed.

At the same time, most FIs are evaluating other digital/mobile wallets solutions in the marketplace, some noting previous or current involvement with Google Wallet and Softcard, to address Android or other OS users. Several FIs are also evaluating the future potential of HCE.

Large and mid-sized FIs may be able to build the interfaces to support Apple Pay (e.g., KeyBank, M&T, PNC, U.S. Bank), but regional and smaller community FIs and credit unions face a different challenge. Smaller FIs must rely on their processors and the card networks to get started and make educated decisions. Many of them are not familiar with the different tokenization schemes, so processors are providing their clients with roadmaps that outline the decisions that need to be made (e.g., build in-house or outsource). However, processors and other third parties wanting to provide

---

service has over 300M mobile identities based on a partnership with the four largest U.S. mobile carriers. Payfone assigns each identity a unique tokenized ID based on the mobile subscriber's phone number, SIM card and account number, and tracks changes in customer use as they are reported to the mobile networks. If the phone is reported lost or stolen, Identity Certainty automatically revokes the mobile ID, and terminates access to apps and services in real time on the individual device. Payment Cards and Mobile. (2014, December 15). *U.S. Banks partners Payfone for mobile authentication*. Retrieved from http://www.paymentscardsandmobile.com/us-banks-partners-payfone-mobile-authentication/.

Apple Pay to their clients (i.e., on behalf of services) must first be approved by Apple, and informed about what is being required and planned.

Initially, many smaller FIs felt pressured to participate in Apple Pay, without having adequate time to perform due diligence on the new payment platform or to carefully review contracts. Sometimes there were conflicts between the risk and marketing departments of the FI, as sales people saw an opportunity to leverage the premium iPhone customer base to use their payment cards.[62] Since Apple Pay transactions use the card linked during provisioning as the default card, FIs also have felt pressure to join the program in an effort for their card to be "top of wallet." Now that the first wave of FIs have implemented Apple Pay, and more information is available on how the process works, other FIs are in a better position to deliberate on what steps they need to take to sign up.[63]

Many credit unions plan to monitor Apple Pay for now, and have opted to participate in the CU Wallet launched in 2013 by the Credit Union Service Organization (CUSO).[64] CU Wallet currently has 87 members and provides the industry's first credit union-driven mobile payment solution using the Paydiant white label platform. One credit union interviewed has been using Google Wallet for nearly two years and plans to adopt CU Wallet by the end of 2015. The credit union's leadership wants to participate in multiple wallets to provide its members with the same services that are offered by the large, national banks. Because their members expect this type of service, they have to satisfy their member needs. They see tokenization as a huge improvement in terms of security and believe it is a proactive step to mitigate the various types of compromises and data breaches in the market, and that once consumers understand the benefit of not using their actual card information adoption will grow.

When building the Apple Pay business case, many FIs consider the number of customers that are likely to upgrade to the iPhone 6 and how many have already upgraded. One FI indicated that a key component in their business case evaluation was to estimate the number of their customers that had iPhone 6 devices. They then factored in growth over the 2014 holidays and estimated higher adoption over the next two years. Another facet to building a business case and forecasting future adoption is to look at how many iPhone 6 devices have been purchased and how many people have provisioned those devices. Currently, only 41.3 percent smartphone users are iPhone users, compared to 53.2 percent for Android.[65] Based on comScore research, iPhone users tend to be more affluent and have higher spending rates.[66]

Having a mobile device capable of initiating an Apple Pay transaction is only part of the business analysis. The other key element is determining where customers will be able to use their

[62] Some smaller FIs perceive that Apple Pay's process of making the first card enrolled the default card provides an advantage to the initial wave of card issuers.
[63] As of March 2015, Apple Pay is supported by 100 financial institutions. Hall, Zac. (2015, March 3). Apple Pay adds 18 more banks and credit unions, 100 institutions supported. *9to5MAC.* Retrieved from http://9to5mac.com/2015/03/03/apple-pay-banks-march/.
[64] For more information, see http://www.cuwallet.com/.
[65] comScore, Inc. (2015, March 4). *ComScore Reports January 2015 U.S. Smartphone Subscriber Market Share*. Retrieved from http://www.comscore.com/Insights/Market-Rankings/comScore-Reports-January-2015-US-Smartphone-Subscriber-Market-Share.
[66] comScore, Inc. (2014). *The U.S. Mobile App Report*. Available for download at https://www.comscore.com/Insights/Data-Mine/iPhone-Users-Earn-Higher-Income-Engage-More-on-Apps-than-Android-Users.

phone. Currently, only an estimated 214,000 POS terminals have NFC capability to accept an Apple Pay transaction.

Other risks also need to be factored into the business case. Most FIs are analyzing the data that Apple tracks and stores, along with the associated risks. For example, the Apple Passbook PAN is not stored in the Apple cloud, but in the TSP's token vault. Furthermore, some FIs are tracking existing fraud rates on customer iTunes accounts. According to our interviews with various stakeholders, iTunes appears to have high transaction volume fraud, although low dollar volume, and most of this fraud stems from purchases of iTunes gift cards.

Payment Processor Experience with Apple Pay

Interviewed payment processors that support Apple Pay for their FI and merchant clients expressed strong support for its use of a static token with cryptogram and Touch ID for authentication. Some of the merchant processors are supporting Apple Pay because their merchant customers believe it will increase their in-app and POS sales. Several processors offer SDKs and APIs to enable merchants and developers to accept Apple Pay transactions (both POS and in-app), and others provide on behalf of services to card issuers and/or security tokenization services to retailers for Apple Pay.

On the merchant/acceptance side, some processors are enabling acceptance at the POS by supporting contactless/NFC readers at merchant locations. They believe that adoption of EMV contactless POS terminals will gain momentum, even among smaller merchants unaware of contactless payments.

Processors for small and mid-sized FIs are trying to ensure that their card issuer clients can participate in Apple Pay now and not be disintermediated by the larger issuers. They do this by providing on behalf of services to card issuers for Apple Pay. They are helping smaller FIs provision tokens in Apple Pay for their customers' cards through connections with the TSPs. Most processors currently play a limited role in the token provisioning decision but most would like to play a larger role in provisioning in the future. These processors view Apple Pay as a game changer for smaller FIs that can help them accelerate their mobile strategy and remain relevant in this space. Furthermore, processors can help to educate many of their client issuers who lack knowledge about tokenization or Apple Pay, but are anxious to learn.

These small and mid-sized FI processors also provide *Yellow Path* authentication services and an 800 number to call for lifecycle management to their clients. One processor reported it has about 5,000 credit and debit clients that could potentially offer Apple Pay, but is waiting for Apple to provide a start date. In the meantime, this processor has created a user guide to help FIs understand the additional authentication, certification, and documentation requirements that need to be completed before going live. They expressed some concerns about additional technical specifications for the lifecycle management process and the ability to service multiple types of wallets (i.e., "How will nuances be supported across wallets or schemes?").

One processor providing Visa and MC on behalf of services to its clients noted that it has implemented about ten card issuers and has over 100 that are either in progress or will soon be active. Another 200-300 card issuer clients have signed contracts with Apple and are moving into the

implementation phase. Because Apple must certify every card issuer, they need to maintain that capacity to keep up with the queue of issuers waiting for certification. The processors initially experienced some inconsistent communications from the card networks and a few implementation setbacks where rules were changed by Visa, MC, and Apple, which required the processor to redesign steps. However, they reported that they have been able to keep up with client demand, driven by when card issuers want to implement Apple Pay. Each card issuer must take a customized approach to implementation due to the different card network requirements so broader adoption of token usage among issuers will take some time.

Although specific volume figures have not been released, processors that are receiving and processing Apple Pay transactions report seeing expected volume growth and have not seen or heard of any problems from either the card issuers or the merchants, including potential issues with returns and chargebacks. Overall, they view the willingness of FIs and merchants to make investments in Apple Pay as positive for the industry.

C. Apple Pay Challenges

Observations from card issuers, networks, processors, and payment technology providers on Apple Pay deployments and growth are generally positive. The industry sees the value of Apple raising the bar for more secure transactions using tokenization and biometrics for authentication, and providing a convenient consumer experience at checkout. Despite the good feedback, there are challenges impacting adoption, such as the lack of a loyalty and rewards program, (although Apple recently announced that it is in development), low consumer demand, limited iPhone 6/6 Plus upgrades, and the lack of repeat usage among current adopters.

Apple Pay only works on selected iOS devices, and does not support users of mobile phones with the Android OS – about half of the U.S. smartphone market. Another obvious challenge for all NFC wallets is the dearth of NFC-enabled POS terminals/merchant acceptance. Apple Pay is available on the same 220,000 contactless terminals that worked with Google Wallet and Softcard.[67] Until there are more merchant venues accepting NFC, volume and growth will be difficult to predict.

IX. Merchant Perspectives on Mobile Commerce and Payment Tokenization

Merchants want to use mobile technology to manage payment choice, protect transaction, account and customer data, and foster a conscious, holistic, and well-managed customer experience. Merchants of all sizes also believe in the potential for mobile to be a very secure and affordable platform that allows them to leverage the cloud and mobile apps, but are also aware of the potential risks of the mobile channel.

Many merchants are eager to leverage digital/mobile technology beyond the payment experience to aid customers in planning their shopping, selecting stores, inviting visits, aiding product selections, incenting and rewarding choices, applying rewards, and facilitating post-checkout

[67] USA Technologies will make Apple Pay available in 200,000 of its vending machines by the end of 2015, and Coca Cola will have it available in over 100,000 of its vending machines also by the end of 2015. See http://www.eater.com/2015/3/9/8176601/apple-pay-100000-coke-machines and http://techcrunch.com/2015/03/09/apple-pay-stats.

functions. While they might accept other wallets (e.g., Apple Pay, Google Wallet, PayPal, etc.) to streamline the customer experience at the point of payment presentment, they want control over other buyer and seller interactions. Merchants want the ability to determine whether or not they accept any individual wallet schemes.[68]

Merchants are concerned that they will not be able to accommodate some use cases in the EMV specification. For example, they need to better understand how they will use a payment token to look up a customer purchase and process a return/chargeback. While they share the card issuers' desire to move away from using the PAN as an identifier for lookups and returns, they are not sure how they will recognize a tokenized transaction from one carrying the PAN.

Such use cases highlight the need for merchant input to the process, as it may require adjustments to merchants' internal processes or modification of the EMV specification. The EMV specification has addressed many of the traditional use cases, but the merchant and EMVCo communities should collaborate more to address differences, particularly since tokenization marks a significant shift in the payments ecosystem.

A. Handling POS and Ecommerce Exceptions

Exception handling in payments is an essential and expensive part of transacting. It often requires knowing considerable detail about the transaction to resolve a customer problem. Furthermore, interactions between multiple parties (e.g., FIs, merchants, networks, and third parties) complicate the ability to effectively resolve some sustaining concerns, such as friendly-fraud.[69]

Merchants tend to establish their own return policies. For example, Amazon customers must print receipts (i.e., voucher) to include with a return sent via mail because Amazon does not have a physical storefront. In other instances, merchants can use an email address to initiate an in-store return. Some POS merchants allow customers to buy online and then use the card number as a look-up reference for in-store returns. This method can create challenges if the customer presents his physical card/number for the return when a token was originally used for the transaction.

Merchants that use PANs to lookup customer information have been encouraged to adopt a transaction ID number or an email address instead. Some merchants are moving away from using card numbers for lookups at POS, but if they continue to use the card number for their online environment and want to deploy tokenization, this defeats the purpose of using tokens as non-payment IDs for look-ups at POS. The reverse is also true. If they continue to use PANs for POS and then only deploy tokenization for ecommerce, they devalue the tokenization approach because the real PANs can still be used to commit fraud. Merchants should look for ways to deploy tokenization in both venues and stop using account numbers for returns and lookups to fully leverage the value of tokenization.

Even prior to tokenization it was considered bad practice for merchants to use the PAN for customer lookups on purchases made with plastic cards, as it exposes the merchant to the risk of data

[68] Visa issued a rule regarding the acceptance of all NFC wallets. The network programs do not distinguish between different mobile wallet solutions, so merchants cannot selectively accept one NFC wallet over another. Visa Business News. (2014, October 30). Contactless payment acceptance requirements. *Systems & Operations | Visa Rules*.

[69] Friendly-fraud occurs when an account-holder denies doing a transaction, or claims family or friends used the account without authorization.

breach and account compromise. This is why many merchants – POS and ecommerce – proceeded to deploy tokens for these purposes.

Large merchants integrate across ecommerce and POS to support backend CRM systems. Their CRM systems store localized account numbers which allow the merchants to look up the customer using the account number as the customer identifier for online purchases. Some merchants use other methods for identification, such as the barcode, which customers can print from a merchant website.

Merchants need to know how the EMVCo tokenization framework will affect different types of refunds, e.g., current (30-day), older (12 months later), or goodwill refunds, and how processors and merchants will get access to tokenization details to manage fraud. Some worry that without more open standards, EMVCo or a card network could independently change a card scheme or format and negatively impact current merchant or third party provider tokenization processes.

While EMVCo maintains that exception handling in Apple Pay and future tokenized wallets will conform to existing merchant processes, merchants cite the inability to easily link the token to the customer's payment account as a major issue that EMVCo has not specifically addressed. However, there is an expectation that consumers might do what they do now—call their FI—and FIs will do what they do now—refer them to merchants, creating confusion for all parties. The FIs and merchants need to coordinate how to procure other data they need from Apple and other payment venues to effectively resolve exceptions.

Some payment processors and gateways consider merchant-centric cross-channel tokenization an important development. Merchants want a token they can use to understand what is happening across their payment channels (e.g., POS, online, and mobile). Tokenization is supporting the market convergence to a cross-channel configuration by expanding its scope from fraud prevention and payment security to encompass a more holistic Know Your Customer (KYC) tool. Processors are trying to figure out how cross-channel tokenization will work for their merchant customers, and consider this change a much bigger issue than Apple Pay.

Many merchants, particularly in the ecommerce space, already have standards and proprietary tokenization solutions that extend beyond payments. Merchants and acquirers have deployed their own ecommerce security tokenization solutions for years, where security is not only a customer and brand issue, but also a fraud liability concern for merchants. They have invested time and resources to create their own tokenization solutions to fill the void in ecommerce security and believe it will be easier to integrate the new payment token specifications into their systems if they are open and interoperable. They also do not want to support a *payment card only* token solution if it requires merchants and processors to assume the costs and liabilities.

B. Merchant Recommendations

The Merchant Advisory Group (MAG)[70] offered several tokenization recommendations to protect against fraud, enhance competition, provide a high level of return for commercial stakeholders, and support modified approaches to the EMVCo framework development process and the payment card networks as outlined below:

- Accredited standards body should own and manage tokenization standards to enable fair representation of all stakeholders, enhance competition, and promote a free market.
- Develop interoperable tokenization standards that also support multi-faceted commerce (e.g., a single tokenization system for payment card data, driver's licenses, passports, or prescription numbers that may be sent as fields necessary for authorizing a transaction or for other purposes).
- Provide an open environment for token management so that companies that meet specific standards and security audits based on accredited standards criteria can become TSPs.
- Require end-to-end tokenization and encryption (i.e., transactions which originate at the POS must be tokenized and/or encrypted completely through to the party that issues the card).
- Limit data use captured through tokenization for security purposes and prohibit secondary use.

X. Proprietary Digital Tokenization Schemes[71]

The use of a token as a digital representation of an account is also highly desirable for cloud-based payment services–both online and in-store. The digital payment/wallet providers that we interviewed have had tokenization schemes in place for several years and have a breadth of experience in deploying these systems for their merchants. Given the breadth and depth of their use, and the importance of these token schemes to the providers' business operations, any new tokenization solutions should be designed to accommodate these schemes without disruption to the operations or excessive costs.

A. Amazon Payments

Amazon is the largest internet-based retailer in the U.S. It is also a third party service provider to many ecommerce merchants for payment processing, cloud, and security tokenization services. It has been using one-time static tokens with dynamic elements to replace the user's PAN for ten years. The Amazon model is an example of a token acting as a surrogate for multiple accounts, including loyalty.

Amazon Payments enables a customer to use payment and shipping information already stored securely in his Amazon account to login and pay conveniently on thousands of merchant websites and

[70] MAG represents about 90 of the largest merchants in the U.S. MAG recommendations on tokenization available at http://www.merchantadvisorygroup.org/docs/default-source/resources/mag-recommendations-on-tokenization_final.pdf?sfvrsn=2.

[71] For details on the Google and PayPal mobile wallet models, see Federal Reserve Banks of Boston and Atlanta (2014, May). *MPIW Security Workgroup Initiative Progress to Date and Current Status*. Available at http://www.bostonfed.org/bankinfo/payment-strategies/publications/2014/mpiw-security-progress-status.pdf.

apps without sharing his credit card credentials. Users store their payment credentials in the Amazon cloud to avoid re-entering them for each purchase. Using *Amazon Payments* ensures that the merchant does not access or store the real customer account credentials/PAN. There are several variations of this payment scheme.

(1) *Checkout by Amazon* is an ecommerce checkout solution used by merchants who sell products directly from their own websites, rather than through Amazon.com, but want users to check-out using information stored with Amazon.

(2) *Log-in and Pay with Amazon* is for customers who may not use a merchant frequently and want to check-out through Amazon. By selecting the *Log-in and Pay with Amazon* button on the merchant's checkout page they are directed to the Amazon app. Amazon processes the transaction on behalf of the merchant and provides the merchant with a record of the payment. (In a different version, the user enters his real PAN in the merchant website, and the merchant passes it to Amazon. Amazon returns a token to the merchant without details of how the user wants to pay or the amount.)

(3) *One-Click*[72] allows users to make purchases directly on the Amazon.com website as customers of Amazon, which serves as the merchant and processes the customers' payments. In this use case, Amazon generates an internal security token to protect the cardholder data stored in its servers and to reduce its PCI footprint.

Amazon tokens combine static and dynamic data. These purpose-driven tokens have limitations similar to EMVCo domain restriction controls for different types of transactions. To provide variability for their merchants, Amazon tokens can carry merchant-specific requirements. One downside to secure, one-time tokens is the trade-off between limited use of the token for payments and inconvenience to users and merchants if it is too restrictive.

Generally, Amazon's tokens do not contain any personal data, so whether the token is dynamic or static, the data is harmless and has no value outside of Amazon's network. For example, Amazon has a card-on-file (CoF) repository and uses ID and password to create a security token for the transaction.

Amazon performs a role similar to that of a TSP for its ecommerce merchants, and views EMVCo, the payment networks, and Apple as competitors. Amazon would like to understand how new implementations of the EMV specification (e.g., Apple Pay) may impact how transactions are passed to Amazon as the merchant, and Amazon as the service provider to other merchants.

[72] One-click buying is the technique of allowing customers to make online purchases with a single click, with the payment information needed to complete the purchase having been entered previously by the user. It allows an online shopper at an internet marketplace to purchase an item without manually inputting billing and shipping information. Instead the buyer can use one-click buying for a predefined address and credit card number to purchase.

B. Google Wallet and Android Pay[73]

Since 2012, Google Wallet has been using a single network token that maps to a user's profile stored in its proprietary cloud with payment data stored on its servers not the mobile device. The current version of Google Wallet supports NFC and HCE. A virtual prepaid MasterCard debit card, issued by Bancorp, is loaded into a user's mobile phone, and serves as a proxy account linked to the actual card credentials stored in the cloud. The proxy is stored in the mobile phone OS (Android KitKat 4.4), not in the SE. Using a virtual prepaid account enables users to add any major credit or debit cards to the wallet, regardless of the card issuer.

Google performs a similar role to that of a TSP under the EMV specification. Whether the user is paying at POS via NFC or online, Google generates the token to the merchant. The transaction is routed to Google for authorization against the user's prepaid stored value account or from a default payment card instrument. Google's ID&V process leverages the user's logged in experience to ensure that it authenticates the user who is receiving the tokens for online or tap and pay use cases. The attributes in the payment bundle submitted to the merchant are dynamic on each transaction; usable only for a single payment, while the token itself is static and may be re-used. Google's risk engine determines how often the token refreshes itself, but the token never lasts more than one year. Because Google is the sole issuer of its tokens it can provide the last 4 digits of the token to allow the user and merchant to resolve exceptions in an NFC transaction.

Google's security model uses a range of methods to address both data-at-rest and in-transit. Tokens require dynamic data elements (cryptograms) to be used within each payment bundle that is submitted for processing. The token issuer's processing system and the locally stored (in mobile phone) data are matched to ensure that the transactions are legitimate. This dynamic coordination between device and cloud ensures a much higher level of security than traditional plastic cards, including the ability to perform real-time verification of the device-based information that allows for significantly greater levels of assurance. In addition, if any of the data elements of a token are compromised at a retailer, the token issuer will be able to implement (and should implement) the necessary safeguards to ensure that the compromised token details cannot be transacted against by fraudsters, similar to domain restriction controls in the EMV specification.

Google views the static or dynamic nature of a token (defined as the 16-digit number) as less relevant than the payment bundle that can be submitted for authorization. In any digital model there should be a dynamic element to the payment bundle for the card issuer to affirm a transaction and manage risk (e.g., CVV, transaction counters, or other variables). The construct of the token and related payment bundle should be sufficient to prevent fraudulent TRs from submitting

[73] Google launched its new mobile payment system, Android Pay, in May 2015. Android Pay builds on the foundation of Apple Pay with the use of fingerprint recognition for in-store and in-app payments. Android Pay, like Google Wallet, will work on all versions of the Android OS back to KitKat, which launched in 2013 and enabled HCE for contactless payments. Google Wallet is being reintroduced as a P2P payment application, for customers to transfer money to each other's debit or bank accounts.

stolen credentials. As long as users can appropriately identify themselves and the transaction in question to the merchant or the card issuer, error resolution processes should be accommodated.

Google's alternative tokenization approach relies on its proprietary risk engine that takes into account a user's profile across Google services, leveraging thousands of variables and signals that they can use to authenticate users and transactions. The key limitation is Google's ability to work for extended periods of time in an offline mode. They have deployed controls to support offline mode for a limited number of transactions but will continue to evolve their security model to allow offline transactions.

Google noted that limiting control (i.e., with the TSP) to only a few industry stakeholders could adversely impact innovation and marketplace competition, potentially keeping the costs of TSP services artificially high and innovation low. Since Google serves as the sole issuer of its tokens, its process does not follow the EMV specification. To the degree that future token deployments support multiple token issuers, Google plans to align itself with industry standards.

Google supports the EMV specification as a good start, particularly in terms of how it outlines several use cases for different types of tokens (e.g., POS vs. online), risks, value, etc. The fact that EMVCo has contemplated a series of use cases that are prevalent in the market today is useful and their ability to anticipate future use cases will be important. Google also sees value in Apple Pay's entry to the market, as any solution that encourages merchants to deploy more contactless terminals benefits all mobile wallet providers.

If Google chooses to adopt network standards for tokens it may need to look to the card networks or issuers to play the TSP role. Google has suggested several guidelines for payment tokenization:

1. *Balanced approach to security and user experience* that recognizes the value that some providers can offer to a tokenized solution with seamless and frictionless commerce at high levels of security using innovative authentication schemes that transcend PIN/fingerprint and use software approaches that leverage all the sensory capabilities of a mobile device and nearby connected devices.

2. *Reduce variability in ID&V (i.e., authentication) approaches* that can lead to customer confusion stemming from different interpretations of risk.

3. *Enable competition for token routing* through models that involve broader and more open availability of token services via the regional EFT (debit) networks or other network providers.

4. *Recognize merchants' role in commerce.* Ensure the merchant community does not bear the cost of implementing solutions that may be passed on to consumers in the form of higher prices.

C. PayPal

PayPal's cloud-based digital wallet enables users to pay from multiple accounts, store and use gift cards, access special offers, and store receipts. PayPal options for authorizing payments with the digital wallet include facial recognition/check-in with photo ID, authorization code/QR code, mobile phone number and PIN, or hands-free.[74] Each method uses tokenization to secure the transaction and payment credentials which are stored in PayPal's proprietary cloud.

PayPal has a robust risk management program with sophisticated risk models and advanced technology to detect, and often predict, suspicious activity to help eliminate identity theft. Tokenization and point-to-point encryption are the primary methods PayPal uses to ensure the security of cloud–based payment models. On the front-end, PayPal uses multifactor authentication, as well as information collected through the enrollment process, such as location-based services (requires user opt-in), and device ID to verify the identity the user.

PayPal's risk models use tokens to analyze user activity. For example, it can analyze use of offline tokens to determine a user's previous activity patterns (e.g., is this a regular purchase, where the user was before the purchase was made, is it physically feasible that the token is being redeemed in a completely different location?). Tokens also have mitigating controls such as the inability to re-use the same token. Because transactions are processed in the PayPal cloud, PayPal knows if an attempt is made to re-use a token, and trying to compromise the token is difficult. The probability of someone being able to guess a token value is very low. To prevent malware from obtaining stored tokens, PayPal reverse engineers how tokens are stored on an encrypted mobile device and assumes that the device is not encrypted, and that the application either encrypts or obfuscates the token.

A user can request a small number of limited-use payment tokens through the PayPal wallet app to pay at POS or other offline venues. The user locally authenticates to the mobile wallet app to access an offline token. The user then provides his token to the merchant either by: (1) scanning a bar code representation of the payment token; or (2) manually entering the surrogate payment card number mapped to the payment token. The POS system transmits the token to PayPal for verification.

In September 2013, PayPal acquired Braintree, an online payment gateway provider. Braintree has 4,000 online merchants and maintains 104 million card accounts which it tokenizes for use at these merchant sites. It tokenizes consumer payment card transactions with pseudo PANs for downstream handling by processors and accepts liability for most of those transactions. Braintree's tokenization service enables merchants to accept messages from PayPal to determine whether or not a transaction is completed, rather than seeing the user's payment credentials.

[74] *Hands-free* uses either geo-location or Beacon, PayPal's version of the BLE communicator to enable a user to automatically check-in at a store, receive deals and information via notifications, and pay for products without swiping a card or showing his mobile phone. *In Store* PayPal allows a user to pay in store (at POS) by entering his mobile phone number as the account and his PayPal PIN into the POS PayPal-enabled merchant reader (the user does not need to have his mobile phone with him).

PayPal acquired Paydiant[75] in March 2015. Paydiant is a white-label wallet provider that enables banks and merchants to apply their brands to the mobile wallet. It uses QR codes at the POS and ATMs, integrates with many different POS systems, and offers APIs that can make its deployments compatible with each other. Paydiant provides the primary wallet infrastructure to the Merchant Customer Exchange (MCX), which is discussed in *Section XI-Other Wallet Token Solutions*, as well as the platform on which the CU Wallet has been developed.[76] Using Paydiant's system, PayPal will be able to provide a white label wallet approach to issuers and merchants.

When a user enrolls in a Paydiant wallet, payment credentials are stored in a secure cloud and linked to a reference ID number stored in the QR code in the mobile phone. To make a purchase, the user either scans his QR code at a POS device, or reads the QR code provided by the POS device on the handset, depending on the deployment configuration. Paydiant creates a "*transaction*" token that combines the reference ID number with unique transaction data, and sends it from the POS or the mobile phone to the cloud. The cloud maps the transaction token and returns an approval code either to the POS device, or to the handset for the user to scan at the POS to complete the transaction. Paydiant has a reported more than one dozen card issuers and merchants who have developed and tested its solution for themselves.

XI. Other Wallet Token Solutions

Several other wallets and their respective approaches to tokenization are worthy of discussion. These include the MCX/CurrentC, Samsung Pay, and Softcard.

A. Merchant Customer Exchange (MCX) and CurrentC

MCX was formed in August 2012 by several of the leading retailers in the U.S. to create a mobile payment application for its CurrentC network that will also support loyalty and rewards programs. The CurrentC wallet is a cloud-based/QR code mobile app that is token-based, using the Paydiant tokenization process described above. CurrentC was written on top of the merchant apps so it will have the same features, and the basic interactions and flows will be consistent, although use cases will be different (e.g., POS check-out vs. fuel pump). MCX plans to integrate the token and the MCX process at the POS to go beyond payments with other services, such as loyalty and rewards. The three goals of the MCX wallet solution are: (1) to create an opportunity for a relationship between the user and merchant; (2) to protect data between the two; and (3) to bring balance to the payment ecosystem.

MCX uses dynamic tokens at several points in the payment process. The user begins with one token (a wallet account ID to use for check-in or aisle purchases) to authenticate to the mobile app so the token knows who the user is. The user can shop and scan purchases. At check-out the user pays by selecting the default or specific method of payment. MCX issues a separate check-out token for the specific transaction. No information is stored on the phone except when the user opens the phone to effect a payment.

---

[75] For details on the Paydiant model, see Federal Reserve Bank of Boston. (2014, May). *MPIW Security Workgroup Initiative Progress to Date and Current Status*. Available at http://www.bostonfed.org/bankinfo/payment-strategies/publications/2014/mpiw-security-progress-status.pdf.

[76] Paydiant's largest merchant programs currently in production are the Subway restaurant chain and Harris Teeter grocery store applications.

The MCX token must be the first token received at check-out. If, for example, a card-branded TSP (black box) token is passed ahead of the MCX token, it will hinder the ability of the merchant or MCX to get the user data they need to enhance customer loyalty programs. Merchants question how EMVCo payment tokens will impact a consistent user experience and whether any solution that involves multiple parties issuing tokens will be simple and compelling for the user.

For support purposes, MCX plans to distribute an SDK that provides the ability for merchants offering CurrentC to call MCX. MCX will record all aspects of the transaction for merchants to examine and provide tagging tools so they can learn how their mobile apps are working and where there are problems.

CurrentC has been in development for two years and is expected to go live in 2015. The launch of Apple Pay in October 2014 created a conflict for some MCX retailers who were already accepting NFC contactless payments at POS (albeit in small volume). Because Apple Pay is NFC-based it works with any NFC-enabled POS retail location by default. This put MCX merchants in the awkward situation of competing with their own pending wallet. As a result, MCX merchants chose to disable the NFC contactless feature and wait for CurrentC to become available. It is not yet understood how CurrentC will co-exist with other wallets at the POS.

B. Samsung Pay

Samsung manufacturers mobile phones that support the Android OS. It has the largest share of the U.S. Android market, and 30 percent of the total U.S. smartphone market, as of 4Q 2014, while Apple has 41.6 percent of the U.S. smartphone market.[77] In February 2015, Samsung acquired LoopPay and announced a new wallet, Samsung Pay, which will include two POS payment platforms: NFC with HCE and LoopPay's magnetic secure transmission (MST). MST enables card data pre-loaded in the mobile phone to be read through magnetic pulses for use at traditional POS magstripe card readers to facilitate contactless POS transactions. LoopPay emulates the physical card by replicating a swiped transaction wirelessly when a user holds the phone over the POS magstripe reader swiping slot to make a purchase.

Samsung Pay will default to NFC if the mobile device detects an NFC field on the POS terminal; otherwise, MST will be used. Samsung Pay will support tokenization for both NFC and LoopPay through Visa and MC tokenization services.[78] Samsung Pay, scheduled to debut in September 2015, will operate on the Samsung Galaxy 6 handset.

[77] comScore MobiLens and Mobile Metrix. (2014). 4Q 2014 Quarterly Report. Available at http://www.comscore.com/Insights/Market-Rankings/comScore-Reports-December-2014-US-Smartphone-Subscriber-Market-Share.

[78] After the Samsung Pay announcement, MC and Visa indicated their tokenization services would support LoopPay.

C. Softcard[79]

Softcard was founded in 2010 by AT&T Mobility, T-Mobile USA, and Verizon Wireless and pioneered NFC-based mobile payments and commerce in the U.S. by offering merchants and consumers a new mobile phone payment option. The Softcard model supported NFC-enabled Android mobile phones with an enhanced SIM card-based secure element (SE) that stored the real PANs of participating banks' customers. Until the Apple Pay launch, Softcard was the only U.S. NFC mobile wallet solution still using an SE in the mobile phone, and only model storing the real PAN, not a token.

In February 2015, Google acquired Softcard technology, intellectual property, and other capabilities that support mobile payments. Given Google's discontinuation of Softcard at the end of March 2015 and the uncertainty of whether Google or other wallet solution providers for Android will use the SE, it is important to briefly explain how the Softcard model used the SE to protect the PAN.[80]

Provisioning a user's account in the Softcard wallet required the user to open his PIN protected Softcard wallet and enter his payment information (i.e., name, card account number, expiration date, CVV, and last four digits of his SSN). Softcard's TSM verified the user's credentials (PAN) with the card issuer and provisioned the encrypted PAN over-the-air (OTA) to the SE in the mobile phone. As an added level of security, only the card issuer had the encryption keys to unlock its portion of the SE. Even Softcard could not access the SE to modify a user's payment credentials.

While Softcard did not tokenize the full PAN stored in the SE, it had elements of tokenization using the dynamic CVV with the payment credentials. To make an NFC mobile payment from the SE, the wallet payment applet contacts the NFC controller, which sends the wallet PIN to the SE to authenticate the user and generate an encrypted one-time dynamic password (dynamic CVC3) to unlock the payment applet. The NFC controller transmits the payment credentials with the dynamic CVV from the SE to the POS terminal. The POS terminal builds an encrypted authorization transaction message and transmits it to the acquirer/processor, which then follows the traditional flow to the network and issuing bank for authorization.[81]

XII. Tokenization in Ecommerce

Because the current ecommerce infrastructure is designed to handle PANs, the question becomes how to migrate PANs to something that meets merchant needs, maintains the value of the information that merchants collect, and is also more secure. Merchant CoF systems contain enough data to initiate and complete an online payment transaction. Data encryption and data base monitoring and protection tools protect the data against unauthorized charges. CoF merchants need a better

[79] For details on the Softcard Mobile Wallet, see Federal Reserve Bank of Boston. (2014, May). *MPIW Security Workgroup Initiative Progress to Date and Current Status*. Available at http://www.bostonfed.org/bankinfo/payment-strategies/publications/2014/mpiw-security-progress-status.pdf.

[80] For more information on how the SE works, see the paper referenced above and Federal Reserve Bank of Boston (2012). *Mobile Phone Technology: "Smarter than We Thought": How Technology Platforms are Securing Mobile Payments in the U.S.* Available at http://www.bostonfed.org/bankinfo/payment-strategies/publications/2012/mobile-phone-technology.pdf.

[81] Softcard supported a form of tokenization for the AmEx Serve prepaid product, in which unique proxy credentials were stored in the SE. Softcard also supported tokenization for merchants offering loyalty programs through its SmartTap solution, which leveraged NFC to enable Softcard Mobile Wallet users to pay, present loyalty cards, and redeem offers in a single transaction and pass a wallet ID (token) with the SmartTap payment information to the merchant to track loyalty and rewards for its customers.

system where the cardholder data is never transferred during the transaction, e.g., tokenization. However, using a cryptogram with a token for an ecommerce payment is more complicated than for POS and will need to be addressed differently, requiring the website to be configured to accept the cryptogram. While the EMV specification does not yet illustrate how tokenization would work for ecommerce transactions in detail, it does not preclude tokenization being applied to the ecommerce use cases, such as digital wallets and CoF.

A. Card-on-File and Multiple Tokens

To replicate the CoF ecommerce environment using tokenization, card networks are contemplating the need for between 50 and 100 tokens per PAN, with a different token for each ecommerce merchant by customer. The number of tokens will be based on consumer behavior and the needs of the TRs (e.g., Google, Apple, and Amazon and acquiring processors). The rationale for such a high volume of tokens per account is to replicate consumer behavior for online purchases. Consumers who frequently purchase online could have over twenty merchants storing their card information on proprietary or third party servers associated with digital wallets across the internet because many consumers prefer not to share their information across all the merchants.

If not managed well by the TSPs, use of multiple tokens for one PAN will create complexity and possibly impact consumer usability. The card networks will also need to determine if multiple tokens per PAN will create operational complexities or capacity issues based on the requirements of the current EMV specification. Wallet providers are trying to address the consumer issue by making the last four digits of the card number and the device account number (token) visible so that the consumer can see that the number on the mobile device is different than the actual PAN. Card networks also provide the last four digits of the PAN to the merchant and include it on the receipt. This is another area where better communication to consumers and incentives to modify consumer behavior will be needed.

Card-on-file merchants and processors need to have the option to leverage tokens and cryptograms in different situations if they want them to perform similar to the way domain restriction controls are used under the EMV specification. For example, online payment providers such as PayPal and Amazon could assign unique tokens linked to the same PAN for different merchant websites, and use the device ID as one way to limit how the token is used similar to domain restriction controls to prevent or detect fraud.

MasterCard plans to solve for ecommerce use cases by upgrading the MasterPass acceptance network in 2015 to accept a tokenized transaction request. Visa announced a tokenization solution for Visa Checkout in February 2015. The card networks want to realize a fully authenticated secure transaction environment for digital channels.

B. 3-D Secure (3DS)

3-D Secure is a secure communication protocol used to enable real-time cardholder authentication directly from the card issuer during an online transaction to improve online transaction security and encourage the growth of ecommerce payments. This authentication is based on a three-domain model (i.e., 3D): (1) acquirer domain (merchant and bank to which money is being paid); (2)

issuer domain (bank which issued the card); and (3) interoperability domain (infrastructure provided by the card scheme, e.g., credit, debit, prepaid, etc. to support the 3DS protocol). The 3DS transaction flow is illustrated in Figure 4.

3-D Secure was launched in 2004 as Verified by Visa, MasterCard Secure Code, and American Express SafeKey. In 2010, static 3DS passwords were replaced with two-factor authentication and one-time passwords (OTPs). However, 3DS was not widely adopted in the U.S for a variety of reasons. The issuing FI had to support the product, the cardholder had to pre-enroll their payment cards and designate their 3DS PIN, and merchants had to sign-up for the service and support it through their websites. Once enrolled, the cardholder was required to enter his 3DS PIN in a pop-up window to checkout from a participating ecommerce retailer's site for every transaction.

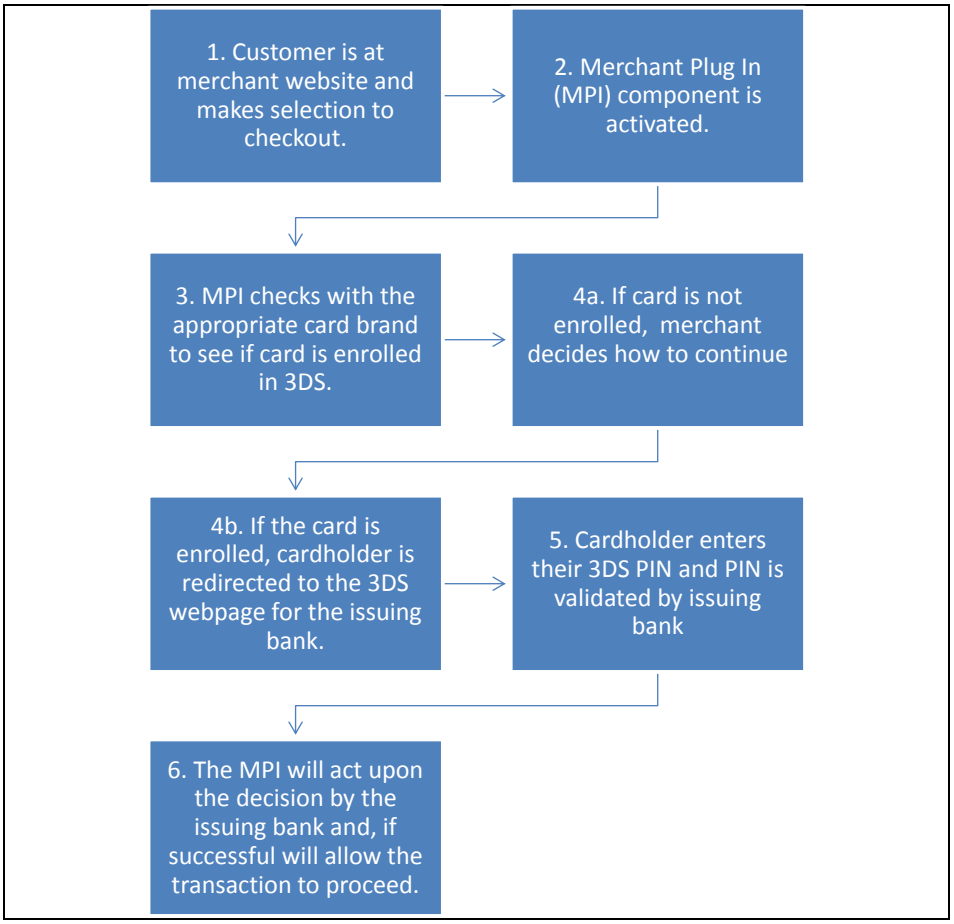
Although online merchants bear the fraud losses, this security method, like other supplemental authentication processes, increases shopping cart abandonment rates resulting in lost sales. For these reasons, merchants have been reluctant to offer 3DS without some recognition of lower risk and card present treatment with lower fees. Alternatively, card issuers have not been inclined to motivate their customers to use 3DS because they are not liable for most of the CNP fraud losses, and consumers have little incentive because of the zero liability commitment of the card networks.

3-D Secure systems are designed to provide a high level of security for online transactions by requesting further payment authentication using 3DS and SSL technology. This provides a standardized and secure method of data exchange over the internet. A transaction using one of the 3DS methods is redirected via an XML message over an SSL connection to the card issuer's website for authorization of the password.

In December 2014, EMVCo assumed oversight of the 3DS authentication solution and plans to modify the protocol into an EMV-based 3DS 2.0 specification, along with a certification program, to be published in 2016.[82] The intent is to address some of the problems merchants faced with the first version in order to alleviate potentially increased CNP fraud post-U.S. EMV chip migration by making 3DS easier for merchants and consumers to use. Possible enhancements include providing a more seamless customer interface to the merchant website, and only requesting the code for higher risk transactions. The updated specification will also incorporate non-payment user ID&V (e.g., IP addresses), while adhering to unique global regulatory requirements. With richer cardholder data there should be fewer password interruptions using a PC for ecommerce. If challenged, a user can identify himself with an OTP or possibly fingerprint verification in the future.

[82] According to a 2013 TSYS whitepaper, only 3 percent of U.S. merchants take part in the 3D Secure service after being available for 10 years. See http://www.tsys.com/Assets/TSYS/downloads/wp_emv-is-not-enough.pdf.

Figure 4. 3-D Secure Transaction Flow



Source: Federal Reserve Bank of Atlanta

XIII. Host Card Emulation (HCE) for Mobile Payments

HCE is a software alternative for enabling NFC mobile payments without requiring an SE in the phone to store payment credentials (or tokens). Instead, HCE stores the payment credentials and cryptographic keys in the secure application memory of the mobile phone OS.

A. Tokenization

Tokenization will be critical to the success and future adoption of HCE because the security of the mobile OS/software environment is not considered as secure as the SE environment. Tokens can be combined with temporary cryptographic keys to create cryptograms using POS terminal transaction data, without having to procure card credentials from the cloud over the mobile network for every transaction. Card issuers will use the cryptograms to authorize mobile transactions. Similar to static tokens, the associated cryptograms in HCE-based transactions are usually good for only single or limited use.

From a pure security perspective, HCE operates in the software environment and needs to be carefully tested because consumers tamper with their phones in ways that cannot be controlled. Also,

NFC is supported by standards through Global Platform, NFC Forum, and ISO. No such standards exist for HCE, yet there is a consumer expectation that the mobile payment will be secure regardless of the technology used.

HCE has fueled increased activity from the major card networks to launch tokenization services because of the higher risk of storing sensitive data or cryptographic keys in phone memory. If HCE is going to be used for mobile payments another level of security, i.e., tokenization, is needed in addition to security provided by the HCE software. Visa and MC plan to use the EMV specification to support their work on HCE. Both have launched HCE trials in the U.S. and elsewhere and may have HCE services ready later in 2015.

AmEx recently released its HCE specification, following a late 2014 trial in Croatia–the first test of HCE on the network. AmEx plans multiple trials of HCE, involving hybrid implementations combining HCE with SEs, as well as implementations relying solely on HCE. Hybrid implementations involve putting tokens on SEs and managing the payment apps in the cloud. AmEx plans to expand HCE service to all of its cardholders sometime in 2015, which will include two million active AmEx, MC, and Visa cards.

Discover plans an HCE pilot in 2015 with its Discover Card unit which may only be NFC and not involve tokens. Discover has completed its HCE specifications and made them available to its Discover Card unit, but has not announced the specifications publically.

Many of the card issuers interviewed recognize that HCE is evolving and consider it to be a viable solution in the longer-term. For now, most FIs are evaluating HCE as a way to accommodate their Android users. Some FIs remain unsure about how HCE will manifest itself to the customer, and assume it will require more time to educate consumers about the security. HCE may satisfy card issuers not inclined to offer an SE-based mobile wallet due to environmental and business complexities, but much uncertainty remains around the mechanics and testing.

B. HCE Challenges and Advantages

Card issuers see several challenges to implementing HCE: 1) methods to encrypt tokens on the device are yet to be determined; 2) use of credentials in the clear in the absence of an SE; and 3) inability to process transactions offline. This creates a circumstance where neither the connection nor the user can be properly validated. Other challenges include how to position offline payments to be competitive[83] and the potential for Android phones to be jail-broken.[84] In effect, the FI may not be handling the application that controls the token request. One FI forces its application owners' developers to cryptographically sign their OS so that it cannot be jail-broken, allowing the FI to maintain the integrity of the application.

Despite some security risks, HCE has several advantages. HCE does not require special hardware nor does it introduce a gateway or another third party into the process, allowing for more

[83] HCE requires management of the offline security while simultaneously managing the security and exposure risk of one-time use tokens without the protection of a hardware chip.

[84] Apple rules do not allow Apple Pay to operate on a jail-broken phone. Android takes a different approach to controlling jail-breaking (rooting), and there have been historic problems with the Google Store which makes one have to assume that the device is compromised and go from there (for Android).

innovation. Implementation does not require contracts (similar to the camera on the mobile phone). HCE offers a level playing field in which anyone can build and provides an open system that allows FIs to control their own destiny.

Some stakeholders are optimistic that an HCE specification will leverage tokenization capability and that card issuers will be able to re-purpose that investment. MC, AmEx, and Visa announced they are writing specifications for HCE Android KitKat, although they are not yet published. The original announcement that the HCE model would store PANs in the cloud without tokenization was not palatable to FIs; although most FIs believe that it can be appropriately managed with tokenization. Support for software-based payments (i.e., HCE) will be needed to promote adoption, which will ultimately be determined by consumer choice.

XIV. Tokenization Landscape Issues

A. Interoperability and Ubiquity Challenges

1. How can the industry address the interoperability and ubiquity challenges of multiple payment tokenization schemes across mobile/digital wallet platforms for POS, mobile, and ecommerce channels?

    a. Currently, several major mobile/digital wallet models dominate the market, including Amazon, Google Wallet/Android Pay, Apple Pay, and PayPal/Paydiant. There are plans to launch others later in 2015–Samsung Pay and MCX/CurrentC. In addition to these models, proprietary/retail mobile applications offer wallets, such as Starbucks, Dunkin Donuts, and LevelUp.
    b. Each platform uses a combination of NFC, SE, HCE, QR code, or other technology and the four major card networks have their own mobile payment solutions for NFC/contactless, HCE, and token services that solution providers must code to.
    c. Given the variability in tokenization schemes, how will acquirers, processors, and non-network parties request tokens, store payment tokens, or tokenize existing tokens (e.g., EMVCo token secondary to merchant-centric security token)?
    d. The process of "tokenizing a token" (mapping a payment token to a security token) needs to be explained to merchants and acquirer/processors.

B. Implementation Issues

1. EMVCo has not released a timetable for when it will publish its TSP requirements and certification plans. Some stakeholders believe that delayed publication of the EMV specification (version 2) may disadvantage qualified companies that want to become TSPs, such as issuer processors that currently deploy large scale risk engines and several payment networks.

2. Non-card network TSPs will still need to obtain token BIN ranges from the card networks when tokens are enabled (as card issuers do today). Merchants want to

understand the costs associated with obtaining token BINs from card issuers and processing tokens.

3. Currently, the Interlink (Visa) and Maestro (MasterCard) debit networks support a tokenization scheme by initiating calls out to the Visa and MC engines, while other processors and networks have provided their own options to enable card issuer compliance with PIN debit dual-routing for mobile POS and in-app payments. However, some stakeholders continue to question how debit routing takes place with Apple Pay.

4. Merchants and debit networks are concerned that TSP/card networks will have access to market intelligence because they will know the EFT/debit network transaction volumes processed over their networks.

C. Security Issues

1. The industry needs more specific formal guidance on the general EMVCo tokenization process and expectations of card issuers and merchant/acquirers in the following areas: (a) provisioning (e.g., to ensure that the ID&V process for authentication is effective); (b) risk scoring to minimize different scoring methods on the same customer account; (c) use of in-app tokenization; (d) potential impacts of using domain restriction controls; (e) what additional data will be added to the ID&V process for tokenization to make decisions about transactions; and (f) whether there will be incremental cost to merchants.

2. How have card issuers, working with Apple, strengthened the Apple Pay provisioning process to address stolen PANs being used to set up Apple Pay accounts?

3. Need to address security gaps and differences in how tokenization is used for different wallet models.

    a. How do tokenization requirements for iOS and Android OS differ? Will Samsung Pay follow the EMVCo protocol?
    b. How will tokenization be applied to HCE and what needs to be done to ensure the same level of security and consistency with the Android/HCE model that is delivered with the Apple Pay SE-based model?
    c. Tokenization solutions to address ecommerce and in-app payments need to be developed or updated (e.g., 3DS).

4. FIs need visibility into where transactions made with their cards occur. If, for example, online wallets mask the identity of the merchant, traditional transaction fraud systems will not work.[85]

[85] Whalen, Elizabeth (2015, March). Tokenization complexity confronts bankers. *BAI Banking Strategies Executive Report*, pp. 15-17. Available at http://www.bankingstrategiesebooks.com/executivereports/innovation_in_payments_2015?pg=8#pg8.

5. How can the industry collectively incent consumers to participate in risk management of the tokenized mobile/digital wallet while not impacting adoption?

    a. Historically, consumers have not been actively engaged in fostering better security because they have been protected by tools such as zero liability policies, with little consequence for risky behaviors.
    b. Tokenization introduces a new level of security but consumers need to understand in a user-friendly way how it works, and where different levels of security might exist where there are inconsistent domain restriction controls or risk scores between card issuers.

D. Standards Opportunities and Challenges

As the U.S. EMV chip migration for cards unfolds, there is an expectation that fraud in both the mobile an ecommerce channels will increase. To mitigate this risk, some industry stakeholders, as noted earlier, are developing a payments tokenization framework. Through this process some challenges have been identified that standards or guidelines might alleviate.

1. The payments tokenization framework should be able to accommodate non-standard merchant/acquirer security tokenization systems.

2. There are no common definitions or a topology for the different types of tokens being used or aimed at this marketplace. For example:

    a. There are two primary types of tokens that can protect transactions in some form: 1) payment tokens for in-transit (e.g., standing-in for a financial transaction); and 2) security tokens, configured for post-authorization and data-at-rest (e.g., in a merchant database), although permutations of both exist.
    b. Tokens can be configured in at least three ways: (1) reusable static form, with some optional extra protections to prevent fraudulent reuse; (2) static-hybrid form, which includes a dynamic cryptogram to make the transaction unique; and (3) dynamic tokens, which are generated uniquely at the source and usable one-time or for a very short duration.

3. There is no formal coordination between proprietary and open standards bodies to address potential incompatibilities and complexities for the industry. No single organization is working on a standard token solution that includes all token types and schemes that might be related to payments and other transaction needs (e.g., loyalty, rewards, etc.).

    a. How can different tokenization schemes operate within a standard framework to minimize changes to merchant/acquirer processing systems?
    b. How will merchants be able to support their business models and continue to use their technology to participate in the marketplace?

XV. Recommendations

A. Strengthen communication between emerging wallet providers (e.g., Apple, Google, etc.) and card issuers, processors, and other industry stakeholders by creating a forum for stakeholders to discuss and resolve issues. Stakeholders would benefit from more details about how various wallet models work behind the scenes, and how tokens are issued on the backend. More technical details will help processors and security providers perform a strong security analysis.

B. Develop industry guidelines or best practices to support use of the EMV Payment Tokenization Specification:

1. Guidelines for a multi-layered security approach. This should include end-to-end or point-to-point encryption, EMV chip/DDA for cards, POS and in-app mobile payments, and 3DS for ecommerce. When used in conjunction they can provide a better value proposition; card issuers and merchants can better assess transaction risks and authenticate cardholder identities online.

2. Standard token definitions and a guide for different stakeholders.

3. Consistent and effective process for risk assurance scoring and assignment of risk values between TSPs and the ID&V process.

4. How tokens are used differently between POS, digital, and mobile channels.

C. Leverage tokenization and "person/device present" concept as an opportunity to revisit the card-present versus CNP framework for liability and pricing.

D. Develop a customer identifier to track consumer end-to-end. Merchants have expressed concerns about the loss of CoF data used to track their customers' purchases and merchant relationships. They want to track the consumer end-to end, for POS, and ecommerce. The card networks and EMVCo[86] are developing a solution that connects the PAN and tokens to a common or master customer identifier, which will not be transaction routable. It will track payment accounts, not consumers. It will link to the card issuer's data center (cloud), associated with a funding account, and authenticated as needed. This will render the PAN useless for fraud, and ensure the issuer is responsible for and handling the authentication. Stakeholders should analyze this development to see how it can improve some of the current limitations of the EMVCo tokenization framework.

E. MPIW as Convener to promote communication and education

1. Communicate issues and concerns raised by MPIW members with EMVCo to help build broad-based acceptance of a token as replacement for the traditional

[86] Smith-Strickland, Kiona. (2015, February 24). Tokenization: Panel looks at costs and benefits of transformative technology. *NFC Times*. This article highlights a panel discussion from the February 2015 Smart Card Alliance Payments Summit that included Marc Lulic with MasterCard. Retrieved from http://nfctimes.com/report/some-will-benefit-others-will-bear-costs-tokenization (Subscription required).

card account. Serve as a bridge between token standards providers and stakeholders (e.g., merchants, FIs, processors, and other payment providers) to collect information and provide feedback on value, usefulness, and issues related to the tokenization platform.

2. Coordinate broad industry participation to develop a standards-based approach that addresses interoperability between payment and security tokenization schemes to help ensure broad acceptance. Convene formal and informal standards bodies to discuss requirements for a comprehensive payment tokenization security solution that determines the framework for multiple, but complementary standards and identifies gaps where open standards could enhance the framework.

3. Provide clarity to the industry/broader market on what tokenization means, how it works, how the various tokenization solutions differ and pros and cons of each through meetings, presentations, briefings, white papers, and other educational materials.

4. Assist the industry in building awareness and coordinating education for consumers and merchants around the benefits of tokenization to drive mobile adoption. Determine how to engage customers in active monitoring of their mobile devices to ensure secure payments.

XVI. Conclusion

The overall security of the payment system continues to be a fundamental concern to all stakeholders – including consumers – and should remain a top priority as the payment landscape advances in the digital and mobile channels. Based on our analysis, interviews, and other discussions with stakeholders, tokenization is viewed as a key component for improving the security of retail payments and protecting payment credentials by removing them from the transaction process. Stakeholders agree that creating payment tokens as part of the consumer account enrollment process is critical to authenticating the identity of the customer and verifying the account credentials, which requires a consistent and strong identification and verification (ID&V) process. The payments industry has lacked a framework for securing payment credentials and the end-to-end mobile payments process until now.

Payment tokenization has transformed the mobile payment landscape by adding the missing layer to the security framework, in conjunction with encryption and the EMV dynamic data authentication (i.e., cryptogram) process. This token-based mobile payment model has also driven new partnerships between financial institutions and mobile wallet providers. While Apple Pay has penetrated the market for iOS users, it has also benefitted mobile wallets using Android (e.g., Google, Samsung); and some have suggested that Apple has become "the rising tide that will lift all boats" in the mobile payments landscape.

Apple Pay has made the use of payment tokenization for retail payments an implementable reality and scalable solution. This concept has provided the industry with a stronger comfort level around security by combining NFC with a token and cryptogram stored in the secure element, and

optional fingerprint authentication. Apple Pay has established a strong foundation for mobile payment security that other wallet solutions should be able to match or surpass.

Payment tokenization still faces a number of issues that must be addressed by the industry as a whole including: (1) establishing a viable standards framework that provides greater inclusivity to all interested payment stakeholders; (2) minimizing the impact on merchant back-end processes, including integration with their security tokenization efforts; and (3) the need for interoperability of cross-channel tokenization and its application in other use cases, such as CNP. However, use of tokenization for retail payments is nascent and all parties must recognize that this is an evolutionary process.

Card networks, card issuers, and merchants should leverage the risk management concepts identified in the EMV specification (e.g., domain restriction controls and token assurance levels). The time is right for the industry to make progress in payment security, but it requires a collaborative approach among industry stakeholders to innovate collectively and monitor the progress of security initiatives, rather than moving to issue any mandates.

Furthermore, payment tokenization has the potential to provide benefits for many stakeholders, including consumers.

1. If enhanced security using tokenization is able to alleviate consumer security concerns, then we will see more growth in mobile payment adoption.
2. Financial institutions now have a complete payment security solution to offer their customers.
3. Merchants benefit from a more secure mobile payment process with removal of the PAN from the transaction data, thereby reducing their risk of potential compromise.
4. While the current model has been developed for retail POS mobile commerce, it can be leveraged for online purchases to drive enhanced security of the ecommerce channel.
5. The payments ecosystem will benefit from the creation of a standards framework to support multiple use cases compatible with a broader industry desire for an open platform.

This paper provides a better understanding of the differences between security and payment tokenization and the impact that the latter is having, and will continue to have, on the payments landscape. It also describes the various tokenization frameworks that exist in the industry from EMVCo, TCH, PCI, and X9 and other proprietary tokenization schemes. The analysis creates a foundation for identifying the gaps and future considerations for interoperability, consistent and open standards, and industry collaboration and partnerships.

Looking ahead, it will be interesting to see how enhanced security methods, such as tokenization, coupled with innovation, help to drive mobile/digital wallet and payment adoption and potentially alter consumer behavior and perceptions about security. The payments industry is changing daily with new technology and new entrants, so it remains to be seen which mobile/digital wallet models will lead the market and how the technology will evolve.