Payment Insecurity

How Visa and Mastercard Use Standard-Setting to Restrict Competition and Thwart Payment Innovation

René M. Pelegero
President and Managing Director

December 2019

An Investigative White Paper

ABSTRACT:

How standards are produced is a critical consideration in modern economies. If decisions about standards creation are made in furtherance of private companies' preferences alone, the public benefit of the standards will be reduced, or even eliminated.

EMVCo is an organization owned by the world's six largest payment card companies that has positioned itself as the representative of the global payments industry. The organization asserts that it produces technical "specifications" needed to ensure interoperability, but those specifications become de facto standards with implications far beyond technical compatibility. In fact, EMVCo has a collusive relationship with its owners. This paper shows a systemic pattern by the card companies to use EMVCo to develop anticompetitive standards that protect the interests of its owners and preempt competition in the market that could lower costs and improve security for businesses and consumers alike.

This paper is the result of an in-depth examination of each of the major areas for which EMVCo is responsible for defining standards, including chip-based credit and debit cards, tokenization of payment data, near-field communication for cards and mobile-device payments, and both the Three-Domain Secure and Secure Remote Commerce standards for online card payments.

RPGC concludes that EMVCo is not the appropriate organization to develop and implement payment specifications that become de-facto standards and strongly recommend that these standards be set by an independent and established open standards-setting body.

NOTICE OF CONFIDENTIALITY

TABLE OF CONTENTS

PART I—INTRODUCTION

1. ABOUT THIS WHITE PAPER

Retail Payments Global Consulting Group was engaged by the Secure Payments Partnership to study and determine whether the U.S. payments industry is best-served by EMVCo as the standards-setting organization for consumer payments.

SPP* represents and advocates on behalf of industries that span the payments system, ranging from retailers to the financial services industry. In keeping with its mission, SPP commissioned RPGC to research whether the standards set by EMVCo unfairly advance card companies' dominance in the United States.† This research also examined whether EMVCo standards deliver the most secure and efficient payment experiences for U.S. consumers and merchants.

The objective of this white paper is to educate readers on the critical role EMVCo plays in how payments are conducted in the United States and how EMVCo impacts the economic, security and competitive aspects of the U.S. payments landscape. The audience for this paper includes merchants, payment service providers, consumer protection and advocacy organizations, policymakers and all other payments industry participants concerned with the welfare and competitiveness of the U.S. payments system.

This research intends to answer the following four questions:

- Is EMVCo furthering the entire U.S. payments industry or simply protecting Visa and Mastercard's market share?
- Is EMVCo capable to develop standards in areas beyond its original charter and are these standards delivering more efficient and secure payments?
- Is the U.S. payments industry's competitive landscape being hurt by allowing EMVCo to establish broad payment standards and should this work be performed by true open standards-setting bodies?

1.1 Background

EMVCo was established in 1999 by Europay (now part of Mastercard), Visa and Mastercard as a global technical body charged with setting interoperability standards for chip cards and chip terminals.‡ Since then, EMVCo's ownership has grown to include four additional card companies – American Express, Discover, Japan's JCB and China's Union Pay – but Visa and Mastercard remain the most influential owners.

EMVCo expanded its scope in 2007 with the publication of a white paper in which it announced its intention to define standards for the mobile contactless payments' infrastructure. EMVCo further expanded its charter in 2013 to "facilitate worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV specifications and related testing processes."[1] In doing so, EMVCo – an organization accountable only to its owners – appointed itself the arbiter of U.S. and global payment standards.

Card payments have experienced explosive growth in the United States over the last ten years. As of

* SPP founding members include the Food Marketing Institute, National Retail Federation, National Association of Convenience Stores, National Grocers Association, First Data's STAR Network, and SHAZAM. SPP advances policies that drive state-of-the-art technologies, competition, and collaboration to continually improve the nation's payment infrastructure, meet the evolving needs of commerce, and provide businesses and consumers with convenience, flexibility, and security in payment options.

† Henceforth, the term card companies will be used to identify the six EMVCo owners: Visa Inc., Mastercard Incorporated, The American Express Company, Discover Financial Services, Inc., JCB Co. Ltd, and Union Pay International,

‡ In 2002, Europay International merged with Mastercard International to form Mastercard, Inc. Today the combined company is known as Mastercard Incorporated.

2017, debit and credit card payments accounted for 54% of all U.S. consumer purchase payments by count and 55% by value, dwarfing even cash (at 35% and 15% respectively), according to a report from the Federal Reserve Bank of Atlanta.[2] The same report states that card payments are seeing robust growth, increasing 10.1% by number and 8.4% by value from 2016 to 2017. Those increases represent an acceleration in overall card payment growth when compared with the previously reported 2015-2016 and 2012-2015 periods.[*3]

Therefore, a study of the organization setting the standards for the payment industry is timely and appropriate. It is timely because of the dominant position of the card companies over this sector of the economy. It is appropriate because standards contribute to public welfare by improving economic efficiency – ensuring compatibility and interoperability. Any standards that give advantage to certain companies over their competitors are a valid concern as this impacts the welfare and competitiveness of the U.S. payments system.

1.2 Methodology

This paper synthesizes a year of research and analysis on the evolution and operations of EMVCo. Its conclusions are derived from an in-depth review of three areas for which EMVCo is now responsible: EMV chip cards, Near Field Communications (NFC) and Tokenization. This paper further looks at upcoming standards such as 3-D Secure 2.0 and Secure Remote Commerce (SRC) which, although not yet fully deployed, have the potential to significantly alter the U.S. payments landscape and have raised many questions and concerns among the U.S. merchant community.[†]

A very important editorial note: EMVCo calls their outputs specifications. Although we acknowledge EMVCo's desire to call their products specifications, we will use the term standards to refer to them because the manner these specifications are implemented, using rules established by the card companies, makes them de facto standards. Because the entire U.S. industry must invest and comply with these specifications, EMVCo specifications, developed jointly with the card brands in an orchestrated strategy, are effectively standards.

The approach used for this research was twofold: First, using publicly available sources and insights from industry experts, we reviewed each standard, noting where and how EMVCo could have produced more open and inclusive standards that would have benefited the overall U.S. payments system. Next, our network of industry experts identified events and other developments that may have brought competition to the card companies and mapped their timing to decisions made by the card companies and EMVCo.

1.3 Organization

Part I includes this introduction, an executive summary, a review of standards and standards-setting organizations, and finally a high-level overview of EMVCo's organization and its specification development processes.

Part II includes an in-depth review of each of the standards for which EMVCo is currently responsible: EMV cards, NFC and tokenization. This in-depth review covers the standard's development process (to the extent that it is documented), discusses the market context in which the standard was developed, explores alternative approaches that would have better served the larger U.S. payments industry, and summarizes how each of these standards benefited the card companies at the expense of competitors, merchants, and consumers.

Part III reviews recently introduced, but not fully implemented, standards such as 3-D Secure 2.0 and Secure Remote Commerce that can significantly disrupt e-commerce and mobile commerce. We will outline the concerns that the U.S. payments community has with regards to these standards and how they can negatively impact the competitiveness

[*] For the 2012-2015 period card payments grew 7.7% by number and 6.5% by volume and, for the 2015-2016 period, they grew 7.8% by number and 6.3% by value

[†] As of the time of this writing, 3-D Secure 2.0 is slowly being adopted, primarily by U.S. merchants selling into Europe and Secure Remote Commerce has been installed at a small number of merchants under the commercial name of "Click to Pay"

of payment solutions in the fastest growing segments of the U.S. economy

Part IV documents our conclusions that EMVCo is not an appropriate organization to develop standards that have such a massive impact on the U.S. payments industry. Our research spotlights the nature of EMVCo as a mechanism for the card companies to collude on the delivery of standards that further their already entrenched market dominance.

2. EXECUTIVE SUMMARY

Understanding the U.S. payments structure and how it has evolved reveals how the card companies compete with other payment networks and how standards have become competitive weapons. The creation of standards is not just a technical matter – politics and market conditions are highly influential in the process, and EMVCo's ownership embeds its own business preferences into the standards-setting process. Because the United States has relatively few regulations with regards to payments (compared to other countries), and there is no governmental or quasi-governmental body that sets baselines for how payments should operate, EMVCo operates as the de facto body that establishes such standards.

Our research reveals an insidious pattern in which the card companies use EMVCo as a tool to maximize their share of transaction volumes: when the card companies feel threatened by competitive pressures or economic challenges, they — or EMVCo supporting their strategies — assume responsibility for the definition of a standard, which results in technical specifications that only benefit the card companies, not the U.S. payments industry at large. EMVCo is an armory for the card companies' arsenal of standards that have been repeatedly brandished against competing payment methods and against merchants' ability to route transactions through unaffiliated debit networks.[*] This paper will show:

- How EMVCo supported Visa's 20-year-plus battle against unaffiliated debit networks, resulting in the implementation of less-secure chip-and-signature EMV cards in the United States rather than the more secure chip-and-PIN cards used elsewhere, limiting the competition that Visa and Mastercard could face from those networks. (Section 6)
- How EMVCo (with support of the card companies) adopted expensive, complex and difficult-to-implement technology such as NFC because it preserved the status quo for the card companies and protected their market share. (Section 7)
- That EMVCo decided to establish tokenization standards that excluded non-card payments, ignoring the work of other standards-setting organizations such as the American National Standards Institute or The Clearing House. EMVCo pushed aside calls for open standards and instead issued a tokenization standard that discriminates against unaffiliated debit networks (Section 8)
- How EMVCo ignored the work of other standards-setting organizations such as the Fast Identity Online (FIDO) Alliance and World Wide Web Consortium (popularly known as W3C) that were developing open authentication standards for both card and non-card systems. Instead, EMVCo is regressing to 3-D Secure, an old standard inherited from the card companies which EMVCo is trying to position as a global authentication standard. 3-D Secure 2.0, as this new standard is being called, is likely to introduce much friction during the checkout process and create obstacles for routing of debit transaction through unaffiliated debit networks. (Section 9)[†]
- That EMVCo has introduced the Secure Remote Commerce standard, which purports to become a new integrated checkout platform for online payment. Neither EMVCo nor the card companies have fully explained and justified the reason for

[*] Unaffiliated debit networks, also known as EFT networks, ATM networks or PIN-based networks, includes networks that were established in the 1970s-1980s to manage automated teller machines and which later expanded into processing transactions at the point of sale using personal identification numbers or PINs. These include networks such as STAR, NYCE, Pulse, and others.

[†] The FIDO ("Fast IDentity Online") Alliance is an open industry association with a focused mission: authentication standards to help reduce the world's over-reliance on passwords. The World Wide Web Consortium (W3C) is an international community where member organizations, a full-time staff, and the public work together to develop Web standards, and which includes the Web Payments Working Group whose charter is to make payments easier and more secure on the Web.

> this standard. Secure Remote Commerce has the potential to be leveraged as competitive pre-emption tool that may limit participation from non-card company payment methods and to hinder merchants' ability to route transactions through unaffiliated debit networks, creating higher dependencies on the card companies and increasing merchants' payment processing costs, as well as potentially violating federal law for debit transactions. (Section 10)

The card companies claim to support open standards. In 2013, Visa's then-CEO Charlie Scharf responded to industry calls for more open standards by saying, "This is an area where everyone needs to work closely together and it's paramount that we ensure transparency, security and integrity so that the integrity of the payment system remains. …It's got to be standards-based, technology-agnostic. It needs to address the needs of everyone globally, not just in the United States".[4]

Given what we have come to know, Scharf's words have proven to be disingenuous. EMVCo portrays itself as a technical specification development organization with no enforcement power over the card companies. Yet, the card companies *are* EMVCo. As will be shown in this paper, both EMVCo's executive committee and its management board are composed of long-term card company employees. Accordingly, it is of little surprise that all its specifications and ensuing de facto standards are designed to meet the needs of the card companies rather than the U.S. payments system as a whole.

EMVCo standards help the card companies maintain their dominance in payment processing volume. They preempt the market by assuming responsibility for other standards, even seizing the work of more qualified standards-setters as their own. EMVCo provides credibility to the card companies' public calls for global payment security standards, all the while directing EMVCo toward standards that provide them with unfair advantages.

EMVCo uses the language of "compatibility," "interoperability" and "secure transactions" but these concepts are belied by EMVCo's own practices. This rhetoric is invoked even though EMVCo or the card companies routinely preempt competing standards and innovations in its quest to maintain EMVCo owners' dominance over the industry.

The next section, Section 3, is a historical primer for non-technical readers who might be unfamiliar with the granularity of payments industry maneuverings, both economic and political. People who are already familiar with the evolution of the U.S. payments industry since the 1980s may choose to rejoin this paper at Section 4.

3. HISTORICAL PRIMER

3.1 U.S. Payments Framework

A payment is an exchange of value. For most people in the United States today, this is represented by money stored in checking or savings accounts at banks or through bank-issued credit lines in the form of credit cards.[*] Banks give their customers payment instruments in the form of checks, credit or debit cards, or user IDs and passwords in order to access their money and credit lines. These instruments have numbers or other identifiers which are the payment credentials exchanged between payers and payees to initiate a payment.[†] To function properly, payment instruments need a clearing and settlement mechanism – a payment network – to deliver the required information to the appropriate parties and transfer funds between payment senders and receivers.

Depending on the instrument, payments are processed by accessing different networks. For example, credit cards access credit lines through Visa, Mastercard, American Express and other credit card networks. Debit cards and prepaid cards access checking or savings accounts either through Visa and Mastercard networks or through the many competing unaffiliated debit networks that operate in the United States such as STAR, NYCE and Pulse. Checks and routing numbers/bank account numbers access bank accounts through check clearing networks or the Automated Clearing House network.

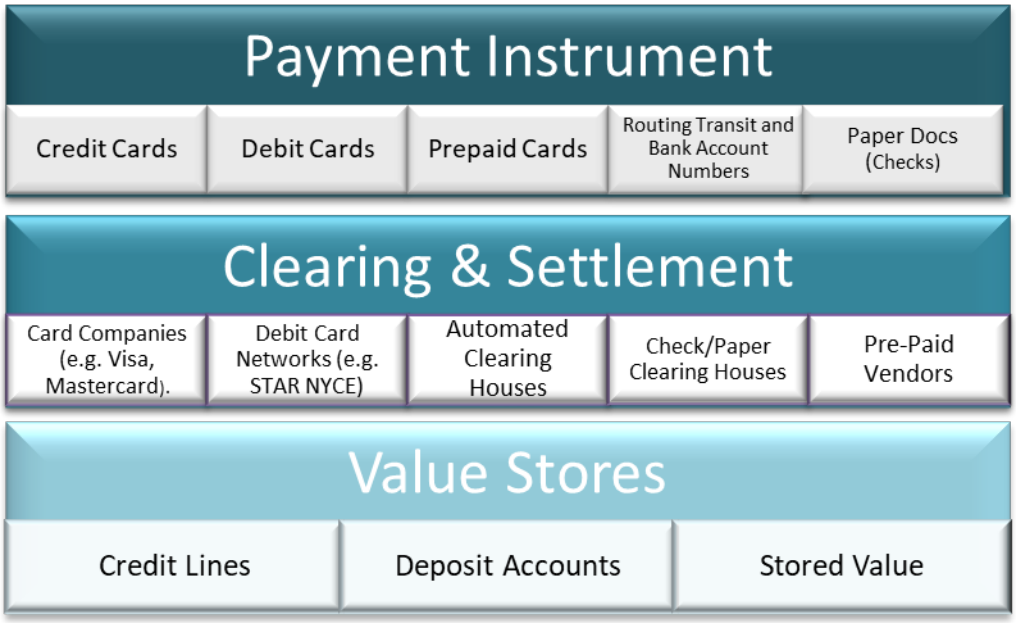

Figure 1 – RPGC's Payments Framework© explains how these components interact with each other

The network used to process the payment defines the standards for accessing it, its cost and the regulations that govern the behavior of the transaction. Thus, network choice is very important for merchants and financial institutions.

3.2 The Need for Standards

Standards are needed for interoperability of bank-issued payment instruments among the networks. For example, checks need a standard representation of check information in a manner that can be read by

[*] To be clear, consumers and businesses also have other stores of value such as retailer credit lines, stored value accounts, etc. This chapter is concerned only with bank accounts and bank credit lines.

[†] For clarification purposes, this paper uses the term *Payment Instrument* to refer to the device or form factor that carries the information allowing the initiation of a payment (e.g. a credit or debit card, a check, mobile phone)

other banks using automated machines.[*] Similarly, debit and credit cards need standards to be accepted by any automated teller machine or point-of-sale device so their information can be transmitted across multiple networks.[†] Thus, standards are critical in deciding who can participate in a payment network. This paper's operating principle is that standards that exclude certain payment instruments or prevent participants from routing payment transactions in a low-cost and efficient manner are not beneficial to the U.S. payments industry and in the case of debit transactions, may violate federal law. To the extent that standards result from a closed or collusive decision-making structure and exclude some participants or payment methods, then antitrust law and policy may be implicated.

3.3 Networks Compete for Transaction Volume

Payment networks – including those run by the card companies and others – compete for transaction volume. The more transactions that flow through a network, the more money and profits the network makes. Because transactions that flow through competing networks do not typically generate revenue for the card companies, maximizing transaction volume is a matter of high priority for them.

The choice of the network processing these transactions also has significant financial implications to merchants and card issuers. The fee paid by merchants for accepting a payment card, sometimes referred as the "swipe fee" by the media, is split into three components: the merchants' processor fees, the card companies' processing fee and interchange which is usually the largest of the three fees that goes to the issuer of the card.[‡] The interchange that issuers get when a debit card is routed through Visa and Mastercard is generally greater than the interchange fee they receive from the unaffiliated debit networks. As a result, the fees paid by merchants are greater when a debit card transaction is routed through Visa and Mastercard than when the same transaction is routed through the unaffiliated debit networks.[§]

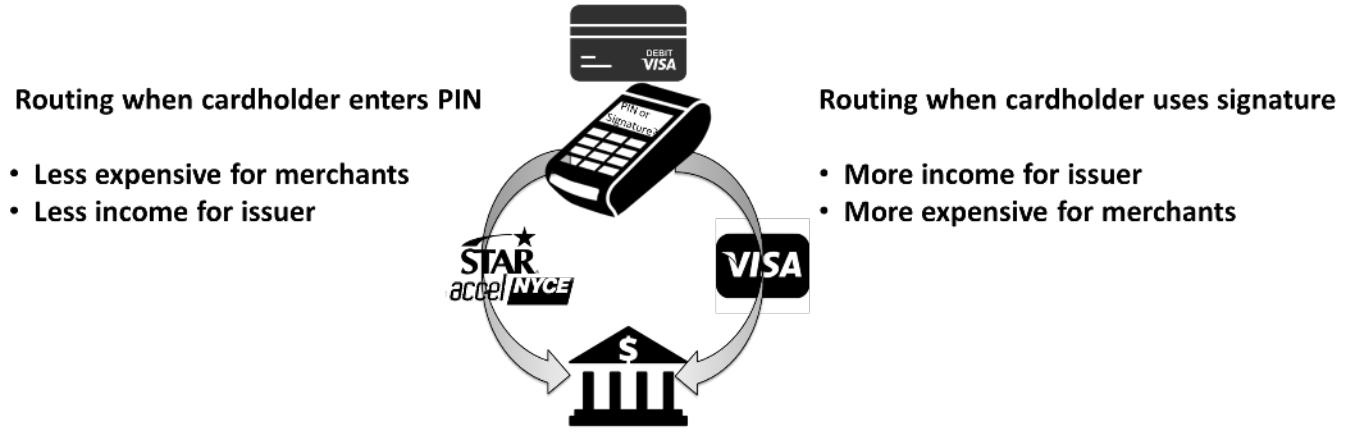

Figure 2 – Debit Card Routing Options

[*] U.S. banks began using the E-13B font developed by American Bankers Association for Magnetic Ink Character Recognition or MICR in 1958. This was adopted by the American National Standards Institute (ANSI) in 1963. MICR enabled checks must meet ANSI standard X9.27-1995 and ANSI X9.7-1990.

[†] Among others, payment cards must comply with ISO/IEC 7813 (properties of financial transaction cards, such as debit or credit cards) and ISO 8583 (a standard for financial transaction messaging for systems that exchange electronic transactions initiated by cardholders using payment cards)

[‡] How interchange and is set is beyond of the scope of this paper. For a more detailed explanation of interchange and how network pricing works we recommend Darryl E. Getter paper "Regulation of Debit Interchange Fees", Congressional Research Service, May 16, 2017, https://fas.org/sgp/crs/misc/R41913.pdf

[§] It should be noted that Visa and Mastercard also accept PIN debit transactions through their Interlink and Maestro networks. However, these networks are considered affiliated to Visa and Mastercard and they do not provide as much pricing differential to merchants as the networks considered to be non-affiliated.

To maintain market share and transaction volume, the networks run by the card companies historically have relied on massive marketing efforts that have made Visa, Mastercard, American Express and Discover household names in the United States and most of the rest of the world. Services such as PayPal also lean heavily on brand recognition to compete for transaction volume.

But the traditional competitors of the card companies – the unaffiliated debit networks as well as non-card payment networks such as the Automated Clearing House and paper-based systems –typically compete without major marketing campaigns. Furthermore, even though U.S. debit cards carry the brand of the debit networks, like STAR or NYCE, over which they can function, Visa and Mastercard require that their brands be featured more prominently on the cards. These practices leave the names of unaffiliated debit networks virtually unknown to most consumers, giving Visa and Mastercard a mindshare monopoly.

Since the 1990s the card companies, primarily Visa, have been engaged in an ongoing battle with the unaffiliated debit networks for transaction volume.[*] The card companies and the banks that issue their cards prefer routing through Visa and Mastercard because it generates more revenue for them. Merchants have preferred routing through the unaffiliated debit networks because of their lower processing fees. In addition, the unaffiliated debit networks offer the additional security option of requiring personal identification numbers, or PINs, to approve a transaction, while the Visa/Mastercard networks historically offered only the less-secure signature option.

Many experts and industry observers have argued that a secret PIN is a more secure authentication method than an easily forged and often-illegible signature, and studies have shown that PIN can substantially reduce fraud compared with signature.[5] While the chip makes it more difficult to create counterfeit payment cards, the National Retail Federation has noted that it does nothing to prevent the fraudulent use of lost or stolen cards. Enabling merchants' option to require the use of a PIN is necessary in order to realize the full advantages of chip cards as has been done in most other countries.

To increase their share of the growing debit market, Visa and Mastercard along with many of their card-issuing banks discouraged cardholders from using PINs. This had the desired effect of increasing transaction volume to Visa's and Mastercard's signature-only processing networks.[†] Further, many issuers had special routing arrangements with Visa and Mastercard that forced merchants to route debit transactions through Visa and Mastercard rather than through the less expensive and more secure PIN-based unaffiliated debit networks.

In 2010, the U.S. Congress passed the Wall Street Reform and Consumer Protection Act, which included a provision, known as the Durbin Amendment, to address rising debit card interchange fees. At the time, debit card interchange was a percentage of the transaction amount and nearly the same as credit card interchange, with an average of about 1.5 percent of the value of the transaction. The Durbin Amendment directed the Federal Reserve Bank to establish limits for debit interchange. These limits, embodied in Regulation II, cap debit interchange at 21 cents plus 1 cent for fraud protection plus 0.05 percent of the transaction amount. The cap, which took effect in 2011, meant that merchants – who were previously charged as much as $1.50 to process a $100 transaction – would typically pay about 25 cents regardless of the amount of a transaction.[‡]

[*] Visa has the largest debit volume of all the card companies. Mastercard has smaller market share and all the other networks are predominantly credit card networks and do not compete for debit volume

[†] During the 1990s-2000s, many Visa and Mastercard Issuers ran advertising campaigns calling for cardholders to "Skip the PIN, and Win!" In order to generate more interchange income, these campaigns sacrificed payments security for higher revenue.

[‡] This cap only applies to debit cards issued by banks with greater than $10 billion in assets. These cards make up approximately 65 percent of all debit cards in the United States. Smaller banks and credit unions still get interchange based on a percentage of the transaction value, estimated at 1.16 percent for 2018.

In addition to limiting the ability of Visa and Mastercard to fix debit interchange fees, the Amendment also required that each debit card must be able to be processed over an unaffiliated debit networks – such as NYCE or STAR —in addition to the Visa/Mastercard networks. Under Durbin, the interchange received by the issuer is the same regardless of the debit network on which the transaction was processed. However, the unaffiliated debit networks offer lower rates for other processing-related fees as well as the option of more secure PIN authentication resulting in less fraud.[*] Network choice is both basic and vital to merchants.

The Durbin Amendment was a massive blow for Visa because it moved significant transaction volume away from its network. Visa was under tremendous pressure from issuers and shareholders to regain that volume.

3.4 EMVCo's Role in Supporting Card Companies' Recapture of Volume

A few months before the Durbin Amendment went into effect, Visa announced its plan to roll out chip cards in the United States. This plan, the U.S. EMV Migration Plan, stated that signature would be the preferred cardholder verification method (referred in the industry as "CVM"). The plan was adopted by the other card companies shortly thereafter and was endorsed by EMVCo even though it delivered a less secure payment authentication method than PIN. EMVCo — despite its claimed commitment to deliver interoperability and acceptance of secure payment transactions — supported Visa's decision for signature authentication of purchases even as merchants and other industry stakeholders demanded PIN.

The Durbin Amendment took effect as the card companies were beginning the rollout of EMV "chip" cards, which culminated in October 2015, when merchants were required to have chip readers in operation or face increased fraud responsibility. The chip card technical specifications established by EMVCo had embedded routing rules that, in combination with Visa's and Mastercard's operating rules, made it very difficult for merchants to route debit cards through unaffiliated debit networks, thus undermining the Durbin Amendment. Through this default setting, Visa and Mastercard could retain transaction volume that might otherwise have shifted to the unaffiliated debit networks.

Not surprisingly, EMVCo did little to address this problem. Instead, the EMV Migration Forum, a cross-industry group, came up with a solution that allowed merchants to recognize and route debit cards through unaffiliated networks. Visa's response to this solution was to require merchants to display to consumers a choice between "Visa Debit" and "U.S. Debit" at checkout. Merchants opposed the Visa requirement because it gave consumers a choice between an unknown name and a familiar name with greater consumer mindshare, likely prompting most consumers to choose the Visa network (this topic is discussed more thoroughly in Section 6.5).

Later, mirroring its attempt to direct payment traffic through the chip-and-signature implementation, EMVCo introduced standards for tokenization that also created obstacles for routing debit card transactions through unaffiliated debit networks (Sections 8). The EMVCo tokenization standard is not based on open standards. The standard does not allow tokenization interoperability among different types of networks and makes it difficult for merchants to choose where tokenized transactions are routed. Worse, no provision was made for the tokenization of bank accounts or any other competing payment method. While these examples are particular to tokenization, they merely represent a small part of EMVCo's pattern of boosting card companies' volumes while hindering that of their competitors at the expense of the security of the entire payments system.

[*] Visa and Mastercard support PIN transactions through their Interlink and Maestro networks but these are more expensive to the merchants than the unaffiliated network. Even today, the preferred choice for the Visa and Mastercard is to route debit transactions via their signature debit networks

4. WHAT IS A STANDARD?

According to the World Trade Organization, a standard is "a document established by consensus that provides rules, guidelines or characteristics for activities or their results."[6] The now-defunct U.S. Office of Technology Assessments issued a study called "Global Standards: Building Blocks for the Future," which said "how standards are set is a matter of some concern because the economic and social stakes in standards are so large. The standards development process must be fair to prevent any single interest from dictating the outcome."[7] Economists see standards as contributing to public welfare by improving economic efficiency.[8] Most standards-setting organizations agree that to achieve these goals, all stakeholders should participate in the development of the standard, the process should be transparent and that information should be openly shared.

Economist Edwin Mansfield calls standards "impure public goods" and emphasizes why it is important that they be developed with a broad stakeholder input:

> *Other goods, like education and standards, are impure public goods. These combine aspects of both public and private goods. Although they serve a private function, there are also public benefits associated with them. Impure public goods may be produced and distributed in the market or collectively through government.* ***How they are produced is a societal choice of significant consequence*** [emphasis added]*…. If decisions about impure public goods are made in the market, on the basis of [corporate] preferences alone, then the public benefits associated with them may not be efficiently produced or equitably distributed.*[9]

As Mansfield shows, privately set standards impact public wellbeing. While there is nothing inherently wrong with private consortia standards, they cause societal harm when they become unfair or biased. For this reason, it is paramount to the U.S. payments industry that a recognized standard-setting body replace the EMVCo which sets standards for the benefit of the card companies.

4.1 Open Standards-Setting Organizations

There are many better-suited organizations to which EMVCo's work could be migrated. In fact, it is likely that the U.S. payments industry and consumers would be better served if different open standards bodies specialized to do the type of work in question.

For instance, the private, non-profit American National Standards Institute or ANSI provides all interested U.S. parties with a neutral venue to work toward common agreements developing U.S. standards. ANSI has an Accredited Standards Committee responsible for developing voluntary open consensus standards for the financial services industry, known as ASCX9. This group has developed a standard called "Protection of Sensitive Payment Card Data - Part 2: Tokenization." This standard, also known as X9.119-2, defines minimum security requirements for implementing tokenization with post-authorization systems to protect sensitive payment card data. As such, ANSI's ASC X9 would a clear candidate to create and maintain open tokenization standards.

New organizations have been established in last decade that address e-commerce and mobile commerce authentication standards. The FIDO Alliance and W3C are industry consortia currently developing open interoperable authentication standards. Although EMVCo claims to work with these organizations, there have been few, if any, deliverables resulting from these cooperation efforts.

These organizations — ANSI, ISO, IEC, W3C and the FIDO Alliance — have consistent approaches to developing standards: open, inclusive, balanced, not dominated by a single-interest category, and consensus-driven. To reaffirm their commitment to open standards, W3C, the Internet Engineering Task Force and the Institute of Electrical and Electronics Engineers Standards Association signed an

agreement to adhere to a set of principles in support of a "modern paradigm for standards." The principles include cooperation, due process, broad consensus, transparency, balance, openness, collective empowerment, availability and voluntary adoption. EMVCo does not follow any of these principles.

4.2 EMVCo: from Consortium Specifications to De Facto Standards

Financed by its member owners, EMVCo is not subject to public oversight, nor is it required to keep records of proceedings during the creation of its standards. It is therefore difficult to obtain systematic information about these processes. Since EMVCo does not offer decision-making roles to other industries, its perspective is biased toward the card companies.

EMVCo asserts that it uses "its own approval and decision-making processes, [and thus] operates separately from the international payment systems which own EMVCo."[10] This is misleading – EMVCo is heavily influenced by its member-owners. There is a long history of card companies developing technologies and turning them over to EMVCo for legitimization as standards. EMVCo says that it is the card companies that "assume the role of defining and issuing products and enforcing EMV compliance for products that carry their respective brands."[11] But trying to differentiate specifications from implementation is a distinction without a difference. Card companies build products in lockstep to implement the specifications that they themselves designed, usually led by Visa. The member-owners implement these specifications consistently and synchronously, making them de facto standards for the United States and other markets in which the card companies' global payment networks dominate.

4.3 Comparing EMVCo with Open Standards-Setting Bodies

Global private regulation has become vastly important in recent decades and is now a phenomenon of considerable social and economic consequence.[12] Outcomes notwithstanding, standards set by consortiums using open processes will always be preferable to closed ones. Though EMVCo's private standards may appear to be irrelevant to broader economic health, payment cards dominate the U.S. payments marketplace to such an extent that these standards negatively impact competition and payments security. Figure 3 shows a comparison between EMVCo and other standards- setting bodies such as W3C and ANSI in terms of membership, mission and decision-making authority.

EMVCo's standards-development process is a closed system operating without any accountability to stakeholders in the U.S. payments system. In contrast with other standards-setting organizations, which advocate openness and inclusivity, EMVCo decisions are effectively made by its six owners, and

	W3C	ANSI	EMVCO
Is active membership (i.e. not just in an advisory capacity) open to all?	Y	Y	N
Is mission and work defined and agreed to by all participating members?	Y	Y	N
Are decision making roles available to all participating members?	Y	Y	N
Are meetings and proceeds documented and open to public review?	Y	Y	N
Are members specialized in the specific technical areas where they contribute to standard development?	Y	Y	Primarily Chip Cards
Appeals process open to all members to resolve differences in standard?	Y	Y	N

Figure 3 – Organizational and Decision-Making Comparison between W3C and ANSI and EMVCo

generally dominated by Visa and Mastercard. Despite claiming to work with other standards-setting bodies, EMVCo sets standards that can only be met by products that were developed by the card companies. Worse, EMVCo has used the guise of global interoperability to co-opt or preempt work being performed by other standards-setting bodies.

The impact of the lack of multi-stakeholder representation in EMVCo is real and measurable. In the United States, the payments industry spends millions of dollars every year complying with standards set by EMVCo and implemented by the card companies as de facto standards. This high level of investment prevents the use of capital to innovate or develop other alternative payment methods. The fact that a standard is enforced by default does not imply it is serviceable, let alone the best.

5. THE EVOLUTION OF EMVCO FROM 2007 TO 2019

In October 2007, EMVCo published a white paper titled "The Role and Scope of EMVCo in Standardizing the Mobile Payments Infrastructure," which stated:

> *There is an increasing need for EMVCo to address and resolve a number of technical infrastructure issues associated with enabling contactless proximity payments via mobile phone handsets. This "technical development" responsibility is in line with* ***EMVCo's traditional role within the payments industry as a technology standards body*** [emphasis added].

EMVCo's "traditional" background and expertise at that point were in chip card deployment, not mobile payments. However, in this paper EMVCo claimed that it should be "the common voice of the payments industry … [assuming] the central role in defining the requirements" for technologies beyond chip cards and presaged greater ambitions. In 2013, EMVCo appointed itself as facilitator of "worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV specifications and related testing processes."[13]

With this expanded scope, EMVCo sought to establish itself as the master and arbiter of all payments technology.

5.1 EMVCo Organization and Decision Making

EMVCo started without any permanent staff. All working groups were led by representatives from the participating card companies, an arrangement that has changed little over time.

Since its inception, EMVCo has been run and operated by its Board of Managers with equal representation from each of the card companies. As it deems appropriate, the board delegates work items, functions and responsibilities to working groups. The Executive Committee provides strategic focus to the board but makes the ultimate decisions.

There is also a Board of Advisors made up of organizations that have an interest in the specifications; most of them processors or technology companies. These are organized as business associates, technical associates, and subscribers. As of July 1 2019, only five out of the 59 EMVCo business associate members were non-payment companies and only one was a traditional merchant. Similarly, only three out of 69 EMVCo technical associate members were not payment companies.[*] Notably, associate members do not have any decision-making power. Figure 4 visualizes EMVCo's entity organization and decision-making process.

[*] To see the current list of both business and technical associates, visit https://www.emvco.com/get-involved/business-associates/ and https://www.emvco.com/get-involved/technical-associates/

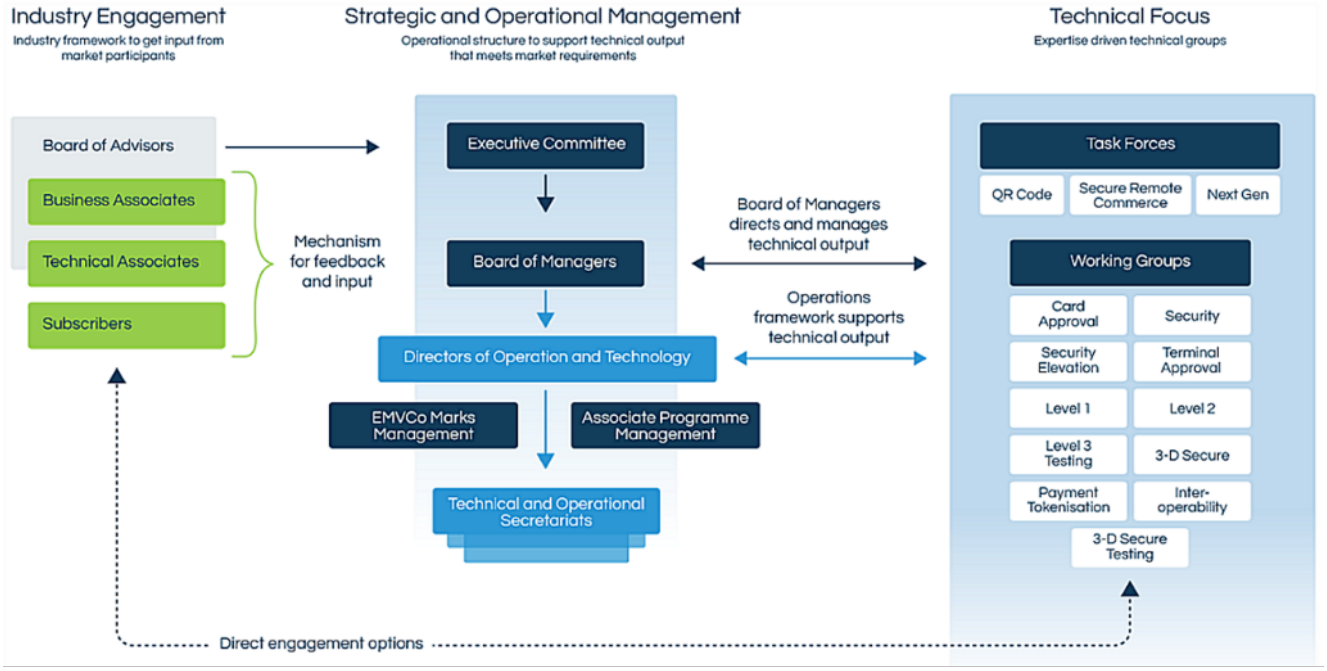

Figure 4 – EMVCo Organizational Structure - 2019

5.2 EMVCo Staffing

Executive Committee members and all Board of Managers members are long-term employees of the card companies. Using publicly available information, we identified several recent chairs of the EMVCo Executive Committee and their respective areas of expertise (Figure 5)*. The chart identifies lifelong card company employees with narrow technical expertise who speak under the pretext of being the "common voice" of the payments industry.

A similar story was found when looking into the background of the current EMVCo Board of Managers (Figure 6), where, again, all members are long-term employees of the card companies.† Given this organizational structure, it is fair to ask where

Name	Period	Employment Company and Length	Experience in
Karteek Patel	2019	17 years with Visa	Processing and Product
Stephanie Ericksen	2018	24 years with Visa	Technology, Chip cards, Risk, Operational Resilience
Jack Pan	2017	3 years with Union Pay and 6 years with Visa	Chip cards
Dave Meadon	2013	17 years with Mastercard	Technology, chip cards
Jim Lee	2011	11 years with Visa and 8 years with JCB	Smartcards and contactless technologies
Tad Fordyce	2009	16 years with Visa	B2B, corporate cards, loyalty, risk and business intelligence products

*Figure 5 – Selected EMVCo Executive Committee Chairs 2009 through 2018**

* EMVCo does not publish an official list of its Executive Committee Chairs nor the length of their tenure. The list presented was compiled from public sources such as press release and media interviews.

† EMVCo's website reports that the Board of Managers consists of two representatives from each owner company

Name	Company	Employment length	Experience in
Christian Aabye	Visa	17 years	Systems Architecture
Robert Burns	Amex	27 years	Technical Architecture
Dhaval Chauhan	Discover	5 years (+ 6 years with Visa)	Mobile payments
Sean Conroy	Amex	32 years	Product Development Chip
Cheryl Mish	Discover	18 years	Payment Security
Jonathan Main	Mastercard	17 years	NFC & mobile devices
Jianhua Ni	Union Pay	1 year (10 years with UL)	Smart cards
Masao Noda	JCB	> 10 years	Chip cards
Jack Pan	Union Pay	3 years (6 years with Visa)	Chip cards
Mark Rigby	Visa	14 years	Chip cards
Patrik Smets	Mastercard	NA	Telecom h/w and s/w design
Junya Tanaka	JCB	17 years	Chip cards

Figure 6 – EMVCo's Board of Managers Members – Early 2019

the allegiances of these individuals lie with regards to their own organizations as compared with the broader charter required of a true industry standards-setting body. By design, EMVCo's Board of Managers is not set up to be impartial third-party experts, instead they are there to represent their company's respective interests.

Perhaps the biggest concern regarding EMVCo as a broader standards-setting body is its failure to include any other stakeholders in its governance structure. Figures 5 and 6 show that there are no other payments industry representatives with extended exposure to any other payment method on either the board or the Executive Committee.

Standardization leader Carl F. Cargill writes that the creation of standards assumes that participants follow rational economic models in their decision making. Yet, he also recognizes that all standard-setting participants are human beings that bring with them their individual backgrounds and biases – professional pride, organizational goals and interests, personal friendships – and this makes standard creation a non-rational human being activity.[14]

With that in mind, our intent in naming the above individuals is not to suggest that they are acting unprofessionally or to attack them personally. Our intent is to demonstrate that EMVCo lacks the neutrality required to develop industry standards through an open, inclusive structure.

Further, EMVCo has refused to work with open standard-setting bodies despite claims that it engages with "other relevant industry bodies."[15] EMVCo has been asked, for example, to include bank account numbers and other forms of payments in the tokenization standard but still limits the standard to work only with products from the card companies.

5.3 Conclusions

Since its 2007 overreach into mobile payments, EMVCo has continued to demonstrate that it is not designed to develop, nor capable of developing, open standards. Its "closed" standards have repeatedly failed to properly address ongoing challenges to payment security and inclusivity at a time when collaborative and competitive standards will be needed to innovate, and most immediately, keep up with upcoming industry developments such

as open banking or "push" payments.* Given its organization, staffing, areas of expertise, internal policies and inclinations, it is unlikely that EMVCo can ever truly be a neutral technology standards body let alone "the common voice of the payments industry."

* Open Banking is a concept being implemented in Europe under the second Payments Services Directive (PSD2) that requires all banks to open APIs to allow accredited Payment Initiators (e.g. merchants, Payment Service providers, etc.) access bank accounts bypassing the card companies; "push" payments are customer-initiated payments where the consumer send payment for goods and services to merchants, sometimes in real-time, using a non-card payment network such as ACH or a Real Time Payment service.

PART II—STANDARDS REVIEW

This part contains an in-depth review of each of the standards for which EMVCo is currently responsible: EMV cards, near field communications and tokenization. This review covers each of these standards' development process (to the extent that it is documented), the market context in which the standard was developed, explore alternative approaches that would have better served the larger U.S. payments industry and how each of these standards benefited the card companies at the expense of competitive networks or methods or payment.

6. EMV CHIP AND PIN (OR SIGNATURE)

6.1 Background on Chip Cards and Risk Management

Prior to the late 1980s, merchants who accepted credit cards were required to telephone a call center to obtain voice authorization if a transaction was above a certain amount, called the "floor limit."* Merchants also had to check a bulletin that listed all reported lost and stolen credit card numbers and could accept a transaction only if the card presented was not in the bulletin. Because bulletins were only updated monthly, thieves had plenty of time to use stolen cards before merchants could be notified. Further, merchants were not equipped to detect forged credit cards despite security features introduced to protect them such as holograms or micro-printing.

To address escalating fraud in the United States, Visa and Mastercard moved to electronically authorize every transaction and eliminate the floor limit practice of exempting those below a certain dollar amount. This process is still in use today. Cards are swiped or inserted in a reader and the information contained in the magnetic stripe or chip is transmitted via telephone lines or over the internet through the Visa or Mastercard networks, to the card issuer for authorization.

The information transmitted contains certain data elements that allow the authorization center to determine, with a reasonable degree of certainty, whether the card presented was forged or reported as lost or stolen. It is critical that a robust and inexpensive telecommunications infrastructure be in place for this approach to work, and the United States had such infrastructure in place at that time.

In Europe, however, a similar approach was not practical due to higher telecommunications costs and lower reliability. Instead, local card companies developed cards enabled with an integrated circuit or chip that could verify the authenticity of a card without the need for a telephone or internet connection. The results were impressive and offered a better alternative to Visa and Mastercard's magnetic-stripe cards. The Carte Bancaire chip card program deployed in France caused fraud to drop from 0.27 percent in 1987 to 0.03 percent in 1995. Similarly, the U.K.'s Association for Payment Clearing Services created the Plastic Fraud Prevention Forum and ran several successful chip-and-PIN trials demonstrating that local card companies were perfectly capable of developing standards for chip cards as a fraud management tool. [16]

In order to protect market share from local card networks, Visa, Mastercard and Europay (which later merged into Mastercard) developed initial technical specifications for smart, secure computer chips that could run verification routines when used in conjunction with PINs. Field trials began in 1996 and,

* The term "credit card" is specifically being used in this section, as in those days, debit cards operated in completely different networks and were protected by PINs. The level of fraud on those cards was a fraction of what banks were experiencing in credit cards. For this reason, credit cards implemented strategies like "floor limits" and "voice authorizations" while debit cards did not.

after successful testing, the first production specification for chip cards was published in 1998. EMVCo was established shortly thereafter.

EMVCo developed standards for chip cards that could work with credit, debit and stored-value cards such as gift cards. In countries that had a national PIN debit network, chip-and-PIN was EMVCo's preferred approach for verifying transactions. But to accommodate countries that did not yet have a robust PIN-debit network such as Russia, China and India, EMVCo compromised and offered the signature option in order to discourage growth of local chip-based card systems and to ensure growth in its members' transaction volumes.[*] So when the card companies took over the role of standards-setting for chip, their motives were clearly rooted in market power, not security.

By 2010, U.K. counterfeit card fraud rates had declined 63 percent following the implementation of chip-and-PIN in 2004.[17] In France, also using chip-and-PIN, the fraud rate from domestic in-person transactions fell by over 50 percent from 2004 to2009 to 0.01 percent. However, these markets also saw a migration of fraud to online commerce and remote purchases channels as well as to cross border transactions where cards issued in these countries were forged and used in countries without EMV deployment. Clearly, chip-and-PIN had helped reduce fraud rates, but all innovations from local card companies were edged out by EMVCo.

6.2 Introduction of Chip Cards in the United States Delayed by Lack of Business Case

Even as chip cards were being rolled out around the world and fraud numbers were being brought under control, the United States remained embroiled in a debate about whether to implement them. Carl Pascarella, then president and CEO of Visa U.S.A. Inc., testified at a 2001 trial in an anti-trust case brought by the Department of Justice against Visa and Mastercard that Visa U.S.A. had "not been able to find a cogent business case or business model" in favor of the chip card.[18] The massive costs involved in converting the U.S. market to chip cards was many times the cost of fraud at the time. This reasoning kept chip cards out of the United States until industry stakeholders voiced concerns in the mid-2000s that the United States was "falling behind."

Still, even as late as 2008, mainstream bankers were skeptical of rolling out chip cards in the United States. Don Rhodes, director of risk management policy at the American Bankers Association, stated that because of the "cost associated with replacing all the checkout terminals … and … because the cost of fraud in the United States is manageable, there is little incentive to change." He continued, "I don't think, based on my discussions with big banks that issue most credit and debit cards, or with card associations, that they envision rolling out so-called chip-and-PIN in the U.S. today."[19] Thus, even though the United States led the world in card fraud at the time, the card companies and their issuers did not feel it was in their best business interests to introduce chip cards at that time.

6.3 Visa and Mastercard Compete with Debit Networks

2010 marked nearly 20 years of battle for debit transaction volume between the card companies, primarily Visa and Mastercard, and the unaffiliated debit networks such as STAR, NYCE and Pulse. Before chip cards, Visa and Mastercard had other strategies for directing debit card transactions to their networks. They introduced their own debit card products, and in 1991 Visa acquired the Interlink debit network. Under its new ownership, Interlink raised interchange fees, driving up costs for merchants but making the network more attractive to banks, which could receive higher revenue from transactions processed over Interlink than they would from transactions on other debit networks. The other debit networks also had to raise their own rates to remain competitive, making banks happy

[*] In 2005 Sberbank in Russia launched its proprietary chip-based scheme called Sberkart which it scuttled in 2010 and replaced it instead with EMV compatible Universal Electronic Cards (PRO100), which itself was scrapped in 2015 for the new Russian payment system Mir.

but driving up costs for merchants and, ultimately, consumers.

During the 2000s, and strictly for revenue motivations, banks issuing Visa and Mastercard cards discouraged cardholders from using a PIN for debit card purchases and encouraged them to sign instead. These campaigns were generically called "skip the PIN and win." In addition, Visa and Mastercard began signing exclusive routing agreements with card issuers requiring merchants to route all their debit card transactions through Visa and Mastercard, further locking in their respective debit market shares.

In 2011, the Durbin Amendment went into effect and banned exclusive routing agreements between card issuers and networks. It required issuers to allow their debit cards to be routed through at least two unaffiliated networks. While the affiliations were technology-based— signature debit versus PIN debit—the distinction signaled was also a branded one: Visa and Mastercard versus the unaffiliated debit networks.

This battle over debit transactions was vital to both groups, as debit card use had overtaken credit card use by 2008. Further, the financial crisis of 2008-2010 significantly reduced credit card use because of consumers' concerns over increasing their debt.[20] Pulse's 2010 Debit Issuer Study found that between 2008 and 2009, the use of PIN debit, largely handled by the unaffiliated debit networks, grew by 13% with an average ticket size of $41 while signature debit transactions, at that time exclusively handled by Visa and Mastercard, increased by 9% with an average ticket of $35.[21]

The provision of the Durbin Amendment that required all debit cards to have at least two unaffiliated networks, along with the new rights given to merchants to decide how to route a transaction (also called "merchant routing rules") had an immediate effect. Interlink volume dropped 54 percent and large debit card issuers saw their average debit card interchange drop from about 44 cents for a typical transaction to 24 cents.

PIN posed an existential threat to Visa and Mastercard's relationships with their largest issuers. Under Durbin, regulated banks (those with over $10 billion in assets) would get the same interchange from a debit card transaction regardless of the network used. Issuers' cost and assessments, however, are generally higher for Visa and Mastercard than for debit networks. Thus, a rational issuer – given the same income from a transaction – would prefer networks that deliver the transaction at a lower cost. PIN was Visa's and Mastercard's enemy because it allowed other networks to compete successfully with Visa and Mastercard for debit transaction volume.

It was within this context that Visa announced its EMV migration program in August 2011.

6.4 Visa Launches Its EMV Migration Plan

Just a few months prior to the Durbin Amendment going into effect, Visa launched its EMV Migration Plan for the United States. That was followed shortly by similar announcements from the other card brands. Surprisingly, given the precedent of requiring PIN in other countries, Visa indicated that its U.S. EMV chip cards would cardholder verification methods, including signature, PIN, and no-signature for low value, low risk transactions rather than chip-and-PIN as deployed in many other countries.[22, 23] All other card brands followed this guidance.

This decision was beneficial to Visa and Mastercard. Under the EMVCo standard, the point-of-sale device uses an "application identifier"* to route transactions according to information encoded in the chip. The AID is used by the POS to select the application that contains the rules governing the

* Application Identifier, or AID, refers to information contained in the Chip. This information includes ways for the POS to identify what kind of card is being used, as well as procedure for routing it.

transaction.[*] AIDs are registered with EMVCo and this information is distributed to all POS device manufacturers to code into their terminals as well as to issuers and card manufacturers. At the time of the announcement, there was no AID for unaffiliated debit networks, meaning that all debit card transactions had to be routed through Visa and Mastercard.

6.5 EMV Preventing Merchant Choices in Debit Card Routing

The proposed EMV migration plan immediately brought to light a major conflict with Durbin's debit card routing regulations. The United States has over a dozen unaffiliated debit networks and some issuers belong to multiple networks to cover different geographic areas; often they change debit network affiliations. Encoding an AID for every network into every card was not practical. Cards would have to be re-issued each time an issuer changed its network affiliation, and the testing and certification process for POS manufacturers would have been lengthy and expensive. The inability to do so under the EMV chip system minimized the number of debit transactions that could be steered to the debit networks, benefitting Visa and Mastercard. Visa's initiative to launch chip cards in the United States threatened to circumvent the Durbin Amendment's requirement for unaffiliated network routing.[†]

Most countries have only one domestic debit network so, encoding an AID for a single debit network is easily done but this was complicated by the number of debit networks in the United States. EMVCo was unable and unwilling to resolve the lack of a debit AID because EMV was never designed for the U.S. market. The EMV Migration Forum — a multi-stakeholder industry association formed to support the U.S. migration to chip technology — appointed itself to resolve the chip debit card problem, resulting on an inelegant solution: the "Common Debit" also called the "U.S. Debit" AID.

The U.S. Debit AID is encoded into every U.S.-issued debit card, which aggregates all the debit networks not affiliated with Visa and Mastercard into one single application.[‡] Importantly, because Visa and Mastercard are on both the Global AID and on the U.S. Debit AID, effectively double-dipping, they can also handle the debit card transaction. For merchants to retain their routing choices they must program their POS devices to select the unaffiliated debit-routing option, but this is far from an ideal solution.

Visa fought back, requiring issuers to prioritize the Visa proprietary AID over the common AID and then demanding that consumer make a choice at the POS between "Visa Debit" and "U.S. Debit." Selecting "Visa Debit" would override merchant routing choice and send the transaction to Visa, while selecting "U.S. Debit" would allow the merchant to route to any network enabled on the card, including Visa. Obviously, consumers had no knowledge about the ramifications of this selection, nor should they need to. Given that the choice between a widely recognized global brand backed by extensive marketing and a name not known or trusted by consumers, these demands highlighted what was important to Visa: steer debit card traffic back to Visa.[§]

Visa's activities asking card issuers and point of sale providers to prioritize its proprietary AID as well as lobbying regulators to mandate consumer choice at the point of sale has given Visa a head start recovering some of its lost debit volume. Ultimately,

[*] For example, Maestro has an AID of A0000000043060 whereas a Mastercard credit or debit has an AID of A0000000041010 and Canada's Inerac has an AID of A0000002771010. This allows the POS device to identify which application it is to work with. The application defines the characteristics of a transaction indicating, for example, what type of Cardholder Verification Method is required from the Cardholder.

[†] Visa's initial intention was to require exclusivity on the chip, relegating the debit networks to the less secure magnetic stripe but this was deemed non-compliant by the Board of Governors of the Federal Reserve System -- https://www.federalreserve.gov/paymentsystems/regii-faqs.htm -- Q1 under Sec. 235.7

[‡] As noted earlier, Visa operates the Interlink network and Mastercard operates the Maestro network, both PIN-based networks, but these are considered "affiliated" for the purposes of Durbin compliance.

[§] US Debit was chosen because the individual debit networks had to share the U.S. Common Debit AID.

the Federal Trade Commission opened an investigation into the matter, and the Federal Reserve again issued an FAQ clarifying that Visa's activities violated the law, so the battle continues even today as merchants fight to enforce this right.*

6.6 EMVCo Failures with EMV Chip Cards

In implementing chip cards in the United States, EMVCo unequivocally failed at its mission to "facilitate worldwide interoperability and acceptance of **secure payment transactions** (emphasis added) by managing and evolving the EMV specifications and related testing processes." It betrayed its own principles by acquiescing to a less-secure verification method by accepting signature as the cardholder verification methos. In addition, all payment credentials remained in-the-clear rather than encrypted during the card-to-POS exchange. That meant that the EMV chip cards were not compliant with requirements set by the Payment Card Industry Security Standards Council, another organization dominated by the credit card companies that sets credit and debit card security standards.†

Furthermore, EMVCo failed to protect the interests of all stakeholders in the U.S. payments industry by agreeing to an aggressive timeline established by Visa which was quickly adopted by the other card companies[24]. Its accelerated timing was surprising considering that it required large monetary investments by merchants and issuing banks at a time when the United States was just recovering from one of the worst financial recessions in its history. Visa gave the U.S. payments industry — one of the most complex, if not the most complex payments system in the world — just over four years to accomplish the massive switch from traditional magnetic-stripe credit cards to chip-based EMV cards. Without any other stakeholders at the table to provide other perspectives, EMVCo went along with the plan.

EMVCo's mismanagement of the certification process also led to delays in EMV terminal certification and deployment, with some merchants saying they waited six months or more for certification of EMV chip card readers they had installed. Without the installations certified, merchants were open to – and suffered - increased fraud liability the same as if they had not installed the equipment at all. And some unscrupulous card-issuing banks allegedly took advantage of the absence of certified chip readers to issue "chargebacks" of transactions against merchants even if the cardholder had not complained of a fraudulent purchase, costing merchants millions of dollars.‡

Visa's and Mastercard's choice of signature debit over PIN debit meant that generating transaction volume was more important than payment security, prioritizing their business interests over the security of the U.S. payments ecosystem. Clearly, EMVCo was a tool used by the card companies to help promote their own strategic objectives to capture market share and increase income.

* In 2016 Kroger Co. sued Visa alleging that Visa threatened Kroger with fines and possibly the loss of the ability to accept Visa debit cards due to its plans for its point-of-sale configuration that would have diverted transactions from Visa's payment network. Visa denied those accusations and the lawsuit was settled out of court in August, 2019, https://www.bizjournals.com/cincinnati/news/2019/08/05/kroger-visa-settle-lawsuit.html

† Payments Card Industry/Data Security Standards (PCI/DSS) is an information security standard for organizations that handle branded credit cards from the major card companies. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council

‡ At a 2016 EMV Migration Forum meeting, a Texas based bank reported they had made $18 Million in chargebacks since liability shift as "Visa had predicted" in a presentation made a few years earlier when banks were looking to Visa for financial remuneration after losing nearly half their debit interchange.

8. NEAR-FIELD COMMUNICATION

8.1 Background

Near-field communication is a technology used in manufacturing, retail and transportation to convey information between two electronic devices in a wireless manner over a short distance, typically just a few inches. Many organizations were involved in setting the underlying standards and data exchange protocols including the International Standards Organization, the International Electrotechnical Commission, the GSM Association and the NFC Forum. The NFC communications protocols were developed by open standards setting bodies and are articulated in ISO/IEC 18092.

NFC began to be used in payments in the late 1990s and early 2000s. Devices and services including Vivo, Bling Nation, the London subway system's Oyster card, Mobil Oil's Speedpass keychain for paying for gasoline at the pump, and contactless PayPass cards from Mastercard and payWave from Visa, used NFC chips to be tapped, touched or waved at NFC-equipped readers. Around 2005-2007, several companies began to incorporate payment functionality into mobile phones by attaching NFC tags to them or by inserting Subscriber Identification Module (SIM) cards with the NFC information. Visa and Mastercard became involved in early pilots to experiment with these new innovations.[*] Nonetheless, one of the outcomes from these pilots was that the card companies soon saw the risk of lost revenue as these new products were based on stored value accounts or set up to directly access bank accounts bypassing the card companies' networks.

8.2 EMVCo Entering Mobile Payments

In October 2007, EMVCo published a white paper titled "The Role and Scope of EMVCo in Standardizing the Mobile Payments Infrastructure," in which EMVCo designated itself as the "representative of the global payments community" and the "common voice of the payments industry on mobile contactless proximity payments standardization." In this paper, EMVCo gave itself the role of definer of standards for mobile contactless payments infrastructure and to consolidate industry standardization efforts.

This was the first time EMVCo looked at enabling payment devices beyond cards and represented the organization's first foray into NFC. During 2007-2010, EMVCo published NFC-related documents that provide insight into EMVCo's continued evolution from a self-appointed standards-setting organization to an instrument to pre-empt the market on behalf of its owners.[†]

The 2007 paper said EMVCo members had agreed "to allow and support the presence of multiple brands, multiple issuers and multiple payment instruments on the same mobile device" to conduct mobile contactless payments regardless of whether the mobile device used a single "secure element" or multiple secure elements to store sensitive information such as bank or payment card account numbers.[‡, 25] This indicated that, at least initially, EMVCo considered including competing brands and methods of payment into its standard.

The story changed in June 2010 with EMVCo's release of the "Contactless Mobile Payment Architecture Overview," where it required that

[*] In 2007 Royal Bank of Scotland launched a "Tap-and-Go" program in partnership with Mastercard in the UK whereas in Atlanta's Philips Arena, NFC developer Philips, Chase, ViVOtech, Cingular and Nokia ran a test in partnership with Visa USA.

[†] These documents include EMVCo Mobile Contactless Payment – Technical Issues and Position Paper (2007), EMVCo Mobile Proximity Contactless Payment FAQ#1 (2008), EMVCo Contactless Mobile Payment Application Activation User Interface (2010), and EMVCo Contactless Mobile Payment Architecture Overview (2010).

[‡] EMVCo describes the Secure Element (SE) as the place where one or more payment applications are hosted, providing a secure area for the protection of the payment assets (e.g. payment data, keys, the payment application code). Secure Element can be deployed as an embedded Hardware Secure Element in mobile phones, on a Universal Integrated Circuit Card (UICC) (i.e. in the physical card), in a removable Hardware Secure Element (e.g. smart card or secure core on multimedia card) not associated with a mobile carrier subscription, or in a Mobile Device Baseband Processor.

"payment credentials" – basically a card's primary account number (colloquially known as the PAN) and expiration date – be held in the secure element and that transmission of that data between the mobile device and point of sale systems must use the NFC communications protocol.[26] By specifying 15-19 digit card numbers and expiration dates as the only acceptable payment instruments the standard blocked potentially innovative and efficient new payment methods that could have been developed if other types of payment instruments had been allowed such as bank routing code and account number, for example.

8.3 EMVCo Selects NFC for Mobile Payments

NFC is just a communication technology. It replaces the "swipe" of a magnetic stripe card with a "tap" of an NFC-enabled mobile phone onto an NFC-enabled point-of-sale device. Whereas the swipe read the primary account number, expiration date and other security data from the card's magnetic stripe, NFC achieves the same objective by transmitting that same information using the NFC communications protocol.

This meant that card companies could move into mobile payments with very little infrastructure investment but, to implement NFC, merchants had to add NFC capabilities to their card swipe POS devices, placing the economic burden on merchants. The rest of the payments' infrastructure remained unchanged because merchants' banks (also known as acquirers) and card-issuing banks had to make minimal if any changes to their systems since, once the cards' information was transmitted from the phone to the POS, transactions behaved just like those initiated by cards.

EMVCo's original architecture had several drawbacks: It was difficult to load the payment credentials onto the secure element (an action called "provisioning"). Only NFC-enabled devices could participate, forcing consumers to acquire NFC-equipped smart phones and obtain NFC-enabled payment cards from participating banks. Under the EMVCo proposed approach, the number of payment instruments that could be provisioned into the secure element was limited to the cards accepted by the mobile phone carrier or manufacturer.

8.4 EMVCo NFC Specification Complicates Merchant Choices in Debit Card Routing

In violation of the Durbin Amendment's requirement that merchants be given the choice of routing debit card transactions over at least two unaffiliated debit networks, the NFC standard omits debit networks that compete with the card companies. The 2011 version of the standard states that the NFC POS or "entry point" software[*] "queries" the card and, based on its response, identifies the list of products supported by the card, the operating system "kernel"[†] they will run with, and their priority relative to one another.[27] Since the "kernels" only support the EMVCo member networks, the standard accommodates only cards from Visa, Mastercard, American Express, Discover, JCB and Union Pay.

In the early NFC implementations such as Isis and Google Wallet, issuers determined the type of cards that were provisioned to the mobile phones.[‡] Very few, if any, loaded debit cards to these wallets.[§] Google addressed this provisioning issue with the introduction of host card emulation that allowed consumers to load whatever card they wanted into Google cloud servers. With this architecture, phones were provisioned with Google-issued pre-paid cards

[*] Entry Point is software in the POS System that is responsible for pre-processing, discovery and selection of a contactless application that is supported by both the card and the reader, activation of the appropriate kernel, handling of outcomes returned by the kernel, including passing selected outcomes to the reader.

[†] The Kernel is the central module of an operating system. In the NFC standard it is the part of the system that provides all the essential services required by the application. EMVCo's standard defines the "card" as any consumer token supporting contactless payment transactions, whether in the form of a payment Chip card, a key fob, a mobile phone, or another form factor.

[‡] Isis was a joint venture between AT&T, T-Mobile and Verizon who ran unsuccessful mobile payment pilots in Salt Lake City and Austin in 2012. The company renamed itself Softcard in 2014 but in 2015 the venture was wound up with intellectual property and some assets acquired by Google for integration into its own Google Wallet.

[§] The number of participating issuers was limited to very large credit card issuers such as J.P. Morgan Chase, Bank of America, Capital One, and American Express that were willing to pay Isis a $3 to $5 per year fee per card fee

that were used to initiate the transaction, but the final charge was made to the consumer's card stored by Google. Still, there was little consumer uptake because of the lack of NFC-equipped phones and point of sale devices.

Since the introduction of Apple Pay, consumers have been able to provision their own cards into the Apple Pay wallet, including debit cards. However, another routing complication arose; because these cards are tokenized before being stored in the iPhone, merchants face challenges when attempting to route these cards through the unaffiliated debit networks. These issues are discussed in greater detail in our analysis of the tokenization standard in Section 8.

In the particularly anticompetitive way that EMVCo drove the industry to NFC technology, EMVCo ignored other communication technologies such as QR codes and also excluded other forms of payment such as direct bank transfer to and from bank accounts, which would have created a competitive threat to the card companies for mobile payments volume. To better grasp the narrowness of the proposed approach, it is useful to review, as we do in the next section, what possible alternatives could have been considered for mobile payments in the United States, and why EMVCo chose to protect its owners rather than act in the interest of innovation, speed and security.

8.5 NFC: A Tool to Prevent Competition

There are alternative communication technologies that allow the exchange of payment credentials between consumers and merchants at the point of sale, which is NFC's sole objective. These include magnetic secure transmission technology originally developed by LoopPay and acquired by Samsung; sound wave technology, which leverages mobile phones' ability to generate and understand sounds; and quick response codes, known in the industry as QR codes.

Beyond the data exchange technology, there are also other available technological solutions for storing payment credentials. Payment credentials such as primary account numbers or other similar numbers required to access an account can be stored in the cloud or in secure servers and can be encrypted or tokenized, which would be an alternative to storage in the phone's secure element. Benefits attained by implementing mobile payments using these alternative technologies would include:

- Compatibility with feature phones and other non-smartphone devices
- Less investment at the point of sale to support mobile payments
- Ease of provisioning payment credentials
- Inability of secure element owners to control or charge rent to payment instrument providers
- Unrestricted debit transaction routing
- Ability to support other payment networks besides those supported by EMVCO's owners
- Flexibility to implement "push" or "pull" payments*
- Access to more than one funding source, including bank accounts rather than just cards

Of these benefits, the last two are the most threatening to the card companies: the ability to introduce other funding sources and the ability to bypass the card companies' networks. Doing so would add competition and allow merchants to avoid the card networks' high fees. EMVCo's choice of NFC for mobile payments preserved Visa's and Mastercard's market positions, and did not enable the best technology.

* A "pull" payment is when the payer (i.e. the buyer) shares payment credentials with the payee and the payee (i.e. the merchant) initiates the transaction. An example of that is a debit card transaction. A "push" payment is when the payee (i.e. the merchant) shares its payment credentials with the payer (i.e. the buyer) and the payer initiates the payment transaction. An example of this would be a bill payment transaction.

The Federal Reserve Bank of Kansas City compared the merits of EMVCo's NFC-based approach to mobile payments with systems such as QR codes and cloud-based approaches such as PayPal. The study showed that NFC compared unfavorably with other technologies in terms of cost, labor and flexibility (Figure 7).[28]

inefficient collaboration between business participants, and was weak from a security standpoint because payment credentials were exchanged unencrypted at the point of sale.

NFC was difficult to adopt because NFC-equipped phones were not widely available until 2014 and

	Technology	NFC	Code-Based	Cloud-Based
1	Examples	Google Wallet, Isis	Starbucks, LevelUp, MCX	PayPal, Square Wallet
2	Required Investment: Consumer	Moderate: NFC-enabled smartphone	Minimal: Smartphone	Minimal: Smartphone
3	Required Investment: Merchant	Significant: NFC-capable POS terminals; Software installation and integration with accounting system	Moderate: QR code scanners; Software installation and integration with account-ing system	Moderate: Software installation and integration with account-ing system
4	Business Models: Participants	Mobile wallet providers; Hardware providers; Tech providers; App vendors; Mobile network opera-tors; Card issuers/Networks; Handset providers	Mobile payment provider; Hardware providers; Tech providers; App vendors	Mobile payment provider; Tech providers; App vendors
5	Business Models: Coordination and Collaboration besides Merchants	Critical	Less important	Less important
6	Funding Sources	Debit, credit, and prepaid cards	Pre-funded accounts or bank accounts	Bank account and/or debit, credit, and prepaid cards

Figure 7 – Mobile Payments' Required Investment, Business Models, and Funding Sources by Technology from "Mobile payments: Merchants' Perspectives," *by Fumiko Hayashi and Terri Bradford.*

8.6 EMVCo's NFC Standard Drawbacks

Despite all of NFC's shortcomings, the card companies and EMVCo promoted this sub-optimal approach which, at that time, was difficult for consumers to adopt, required expensive and most consumers had yet to acquire one. In addition, NFC required merchants to make expensive equipment upgrades. Few contactless cards were initially available and even fewer cards were loaded to NFC wallets such as Isis and Google Wallet. Prior

to the deployment of EMV in 2015, merchants had to buy and deploy expensive NFC-equipped devices at a time when the industry was already gearing up for a massive replacement of POS devices in support of chip card introduction. Rather than facilitating collaboration from all parties, EMVCo created an unfavorable environment for competing mobile payment methods for the sake of enhancing card companies' market share.*

More importantly, EMVCo's NFC standard had major security issues. As noted earlier, the data-exchange of payment credentials between mobile phones and POS devices was unencrypted. Card numbers stored in the secure element were vulnerable to many hacking techniques including malware and "man in the middle" attacks.†

Meanwhile, QR codes ascended to primacy in mobile payments: Starbucks and many other loyalty-based applications made huge inroads using them. The Clearing House ran a pilot using QR codes and tokens as alternatives to secure elements in mobile phones. In late 2015, the largest U.S. card issuer introduced Chase Pay using this technology; Walmart introduced its wallet, Walmart Pay, which also uses QR codes.

8.7 EMVCo's QR Code Standards

QR-code payments were a clear alternative to NFC. Many consumers and merchants found QR codes – the two-dimensional "matrix" bar codes that smartphones can scan to obtain additional information about a product – appealing because all they needed were phones capable of reading the codes. EMVCo kept pushing NFC, however, until issuers in Asia pressured card companies to support QR codes. EMVCo eventually released two QR code standards in July 2017, one for a "consumer-presented" mode and the other for a "merchant-presented" mode.

In the QR Code consumer-presented mode, the funding account can only be attached to "credentials associated with their EMV card previously provisioned to their device."[29] In other words, the QR code can only be generated from EMVCo payment cards. There is no support for any other type of payment instrument such as bank routing and account numbers or private label cards. The specification also assumes that all transactions are processed through the card companies' networks, just as if they were NFC-initiated at the point of sale. By doing so, the QR code consumer-presented standard blocked potential new competitors and technologies from entering the market.

The QR Code merchant-presented mode erects hurdles against competition as well. That mode provides several fields to enter merchants' accounts, which can be in different formats based on the card company or the merchant's "acquiring" bank that processes payments.‡,[30] This standard falls in line with EMVCo's pattern of driving all transactions to be processed through the card companies' networks and obstructing the possibility of these transactions to be processed through alternative payment networks such as clearing houses or unaffiliated debit networks.

8.8 EMVCo's NFC Specification and Apple Pay

In 2011-2012, Apple, working together with Visa, Mastercard and American Express developed a tokenization system that protected the payment credentials during the information exchange between the mobile phone and the POS device. This

* At the time of the NFC specification release and the introduction of products such as Isis or Google Wallet (2010) there was no EMV requirement for the United States. Thus, all POS were card swipe based. Even when new EMV devices were introduced, not all of them came equipped with both EMV and NFC as this was an additional feature that increased the device's cost

† Malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. Malware is used by cybercriminals to target point of sale and payment terminals with the intent to obtain credit card and debit card information. Man-in-the-middle is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other

‡ Merchants accounts with their acquirers are called "Merchant IDs" or "MIDs". Each acquirer has a different format for their MIDs and the templates provide for this variety but these templates are not intended to be used for the entry of bank routing and bank account numbers

system was extended to protect the payment credentials all the way to the networks, launching the concept of "network tokens." After their work with Apple, the card companies passed their proprietary designs to EMVCo to build a specification around them, making NFC a part of EMVCo's design for an integrated payments platform.*

8.9 EMVCo Failures with NFC

Designating itself as "common voice of the payments industry" was a self-serving move on the part of EMVCo. Rather than addressing common concerns like security and interoperability, EMVCo has repeatedly ignored the best interests of the mobile payments system. EMVCo's choices around NFC preempted the market of competitors instead of improving "interoperability and… secure payment transactions". The result was deficient in many areas:

- EMVCo's approach for NFC was cumbersome, unwieldly and ignored the burdens placed on consumers and merchants. It required extensive collaboration between business participants in which they participated reluctantly and, in the end, only nominally.
- EMVCo betrayed its own charter to provide safe payments by introducing a specification that was weak from a security perspective (until the work with Apple Pay offered a tokenization solution).
- EMVCo's selection of secure elements as the account number storage location preserved the existing infrastructure and card company dominance.
- EMVCo did not incorporate alternatives such as cloud-stored payment credentials, which could support alternative payment instruments and systems in competition with EMVCo owners.
- EMVCo's QR code specifications support EMV the card companies' cards as the only payment instruments and do not support any payment method that could possibly compete with EMVCo owners.

The EMVCo NFC standard is another example of EMVCo pre-empting competition, creating barriers to entry and increasing complexity for both merchants and consumers, all for the sake of increased market share for its owners and at the expense of secure payments. EMVCo continues to demonstrate – despite its claims of being the "representative of the global payments community" – that it will not create specifications that benefit the entire payments industry.

Allowing EMVCo to "assume the central role in defining the requirements for an EMV mobile contactless payments infrastructure" does not serve the U.S. payments industry or the global payments industry.

* In August 2011 Visa laid out a vision that merges contact (Chip cards) and contactless (NFC-enabled devices) into a single platform with Secure Remote Commerce (SRC) all integrated into one single infrastructure with Tokenization and 3-D Secure technologies

9. TOKENIZATION

9.1 Background

In the payments industry, tokenization is the process of replacing sensitive account credentials (e.g. a card's primary account number) with a random string of numbers. These strings, called "tokens," unlike encrypted numbers, are generated in a manner that cannot be mathematically reversed to obtain the primary account number. Tokens are therefore safer than encryption because they cannot be reverse engineered making them useless to fraudsters.

EMVCo did not pursue tokenization until 2014. As early as 1998, however, e-commerce merchants were using tokens to hide primary account numbers from being used in-the-clear by their own internal systems. In 2010, acquirers and payment processors began to offer security token services and token "vaults." Through these services, merchants can mitigate PCI Data Security Standards compliance burdens as the card's primary account numbers are stored outside of the merchants' servers.

The card companies, on the other hand, were slow and late to the get into tokenization. The first mention of a token from the card companies was in October 2009, when Visa released its "Best Practices for Data Field Encryption Version 1.0." In this document, Visa said that if a primary account number is needed after authorization, "a single-use or multi-use transaction ID or token should be used instead."[31] Visa advocated for tokenization of the primary account number in its release of "Visa Best Practices for Tokenization Version 1.0" on July 14, 2010.[32] The PCI Security Standards Council released its own tokenization guidelines a year later in August 2011. It is a telling example of Visa's influence over standards and standards-setting organizations that sections of the PCI document are copied verbatim from Visa's best practices document. This should not be surprising, however, as the PCI Security Standards Council is led by an Executive Committee composed of representative from five of the six EMVCo owners (Union Pay is not listed as participating).

9.2 Standards-Setting Organizations Developing Open Tokenization Standards

At the time, other organizations were developing open standards for tokenization, including ANSI's ASC X9.119 and The Clearing House's Secure Token Exchange program. These organizations were proposing tokenization standards that could be used for cards *and* bank account numbers, supported by multiple data-exchange technologies such as QR codes, NFC and dynamic tokens.

TCH's Secure Token Exchange launched in 2012 and started its pilot in 2013. Recognizing that card companies' participation was ultimately needed to achieve market scale, TCH reached out to them. David Fortney, TCH's senior vice president of product development and management, testified before Congress in March 2014:

> *The only way to gain broad adoption of tokenization and ensure a consistent customer experience is to develop an open tokenization standard. Open standards promote innovation and allow customers and merchants to choose the point-of-sale technology that works best for them. But it will require banks, merchants, networks and processors to work together to accomplish these goals.*[33]

TCH called for an open tokenization standard even while EMVCo was beginning its work. In Fortney's view, a truly open standard would involve choice for merchants and consumers, including choice of payment method. TCH recognized the dominance of the card companies in the U.S. payments industry, and that no compelling standard could be developed without their participation.

Shortly after Fortney's testimony, Charlie Scharf, Visa's CEO from 2012 to 2016, responded to industry groups that were calling for open tokenization with the following statement:

> *This is an area where everyone needs to work closely together and*

> *it's paramount that we ensure transparency, security, and integrity so that the integrity of the payment system remains. …It's got to be standards-based, technology-agnostic. It needs to address the needs of everyone globally, not just in the United States.*[34]

Although Scharf appeared to support Fortney's position, EMVCo and the card companies did not work with TCH or ANSI. Instead, they developed their own tokenization standard that was closed to other forms of payment such as bank accounts, private label credit cards and any other alternative method of payment. Any card company rhetoric around openness, collaboration and inclusion was simply that: empty rhetoric, devoid of intent.

9.3 Industry Calls for Open Standards

With so many initiatives for tokenization standardization under way, the Secure Remote Payments Council, which represents unaffiliated debit networks, released a statement the week of July 24, 2014 asking payment industry stakeholders for a collaborative approach in the creation of open tokenization standards.*

The National Retail Federation, Food Marketing Institute, Merchant Advisory Group, National Association of Convenience Stores, National Grocers Association, National Restaurant Association and Retail Industry Leaders Association released a similar announcement on July 28, 2014.[35] These parties called for open standards and requested that work be migrated away from EMVCo to a true standards organization such as ISO or ANSI. Doing so would enable all industry stakeholders to compete equally and support tokenization for all uses, networks and brands in a manner agreed upon by all. Unsurprisingly, the card companies and EMVCo did not migrate this work to a more inclusive and transparent organization, presumably because their focus was to promote their cards as the dominant payment mechanisms, not to promote competition or more secure payments.

9.4 Apple Pay's Role in Tokenization

In 2012-2013 Visa, Mastercard and American Express worked with Apple to expand the concept of tokenization to provide end-to-end protection of payment credentials, resulting in the beginning of "network tokens." Apple combined tokenization with biometric security – first fingerprint readers on its phones and then facial recognition – which

* The Secure Remote Payments Council (SRPC) is a cross-industry trade association dedicated to the growth, development and market adoption of debit-based internet e-Commerce and mobile channel payment methods that meet or exceed the security standards for PIN-based card-present payments. SRCP's definition of debit means any device that accesses a checking or deposit account (or prepaid debit account) including: Card (Signature or PIN), ACH Debit, E-Check, Push-Credit, Chip Device, USB Device and alternative payment instruments

augmented the security of EMVCo's original specification.*

As the work with Apple was wrapping up in October 2013, Visa, Mastercard and American Express jointly announced a new framework, with the shared goal "to enhance the security of digital payments and simplify the purchasing experience when shopping on a mobile phone, tablet, personal computer or other smart device."[36] That announcement was made just three months after TCH released its own comprehensive open tokenization specifications. The key goals of this newer card company tokenization framework were to:

- Ensure broad-based acceptance of a token as replacement for the traditional primary card account number
- Enable all participants in the existing system to route and pass through the payment token
- Improve cardholder security with tokens that are limited for use in specific environments[37]

In contradiction of these principles, the resulting tokenization specifications were proprietary and only applicable to the card companies' credit and debit cards. Although the card companies claim input of "many stakeholders, particularly card issuers and merchants," no merchant can be identified in the documentation and consumer groups were notably missing.

In lockstep with the launch of Apple Pay in October 2014, Visa and Mastercard launched their own token services: Visa Tokenization Services and the Mastercard Digital Enablement Service. Visa and Mastercard began to use tokenization to give their digital wallets a competitive advantage rather than as a universal security standard.†

9.5 EMVCo Takes Ownership of Card Companies' Tokenization

Up until 2014, the card companies' tokenization services were proprietary and directly performed by the card companies. Around that time, the card companies granted EMVCo their intellectual property with the explicit purpose of formalizing it as an EMVCo standard. Almost overnight, EMVCo

* Different from Google Wallet, cardholders provisioned the card number themselves by entering the card number and other information directly into the iPhone (or loading it from their iTunes accounts). Cards had to be from participating issuers that had agreed to pay Apple a percentage of the interchange generated by these cards. In the enrollment process, Apple Pay sends the card number along with other device and consumer related information (e.g. device name, iTunes purchasing history) to the card company for tokenization. The card company, acting as the Token Service Provider or TSP, sends the information to the card issuer for approval and further cardholder authentication. Upon authentication, the TSP issues a Network Token and a unique shared key that is returned to Apple Pay for storing in the iPhone's Secure Element. This token is linked with the device to create a strong association between the device and the token, meaning that payments initiated by that token could only originate from that specific iPhone (and, of course, the Apple Pay application could only be launched by the owner of the iPhone via fingerprint authentication or a PIN). During the purchase process, the Apple Pay application authenticates the phone user via fingerprint or PIN. Apple Pay then generates an authorization cryptogram that that can only be created by that particular iPhone and which Apple Pay transmits to the POS device. The merchant's POS sends the cryptogram to the acquirer, who forwards it to the card company's TSP. The TSP decrypts the cryptogram, validates its authenticity, and detokenizes the provided token back to the original primary account number and passes that information to the issuer for authorization.

† Under a token interchange arrangement, Visa can get tokens from Mastercard for Mastercard cards stored in its Visa Checkout wallet and Mastercard can get tokens from Visa for Visa cards stored in its Masterpass wallet. Both schemes also opened their Token Service Providers or TSP services to third party wallets (e.g. Android, Samsung), as long as the tokens passed through Mastercard's Digital Enablement Service and Visa's Token Service. This is a key point because these tokens (now called "Network Tokens" to differentiate them from tokens generated by PSPs and gateways, called "PCI Tokens") can only be detokenized by the card companies' TSP.

published a fully developed "Technical Framework" in 2014 with no bulletins, lead time or third-party involvement of any kind.[38]

The framework document essentially echoed the work done for Apple Pay and positioned it as a "standard" even though EMVCo conceded that many important issues remained unresolved, such as whether tokens could be reused because of the limited number of bank identification numbers available for tokenization.* Figures 8 and 9 show the sudden appearance of a fully formed tokenization specification (Version 1.0), using web archives to revisit EMVCo's site in 2014, when these standards were released.†

Although EMVCO does not generally release information about its internal proceedings and decision making, its web site contains some information on its work. Examples of these documents are draft standards which are normally shared and posted during the development process. EMVCo also posts notices and bulletins that are issued prior to the release of a final specification. None of that information was available during the process of developing the tokenization standard.

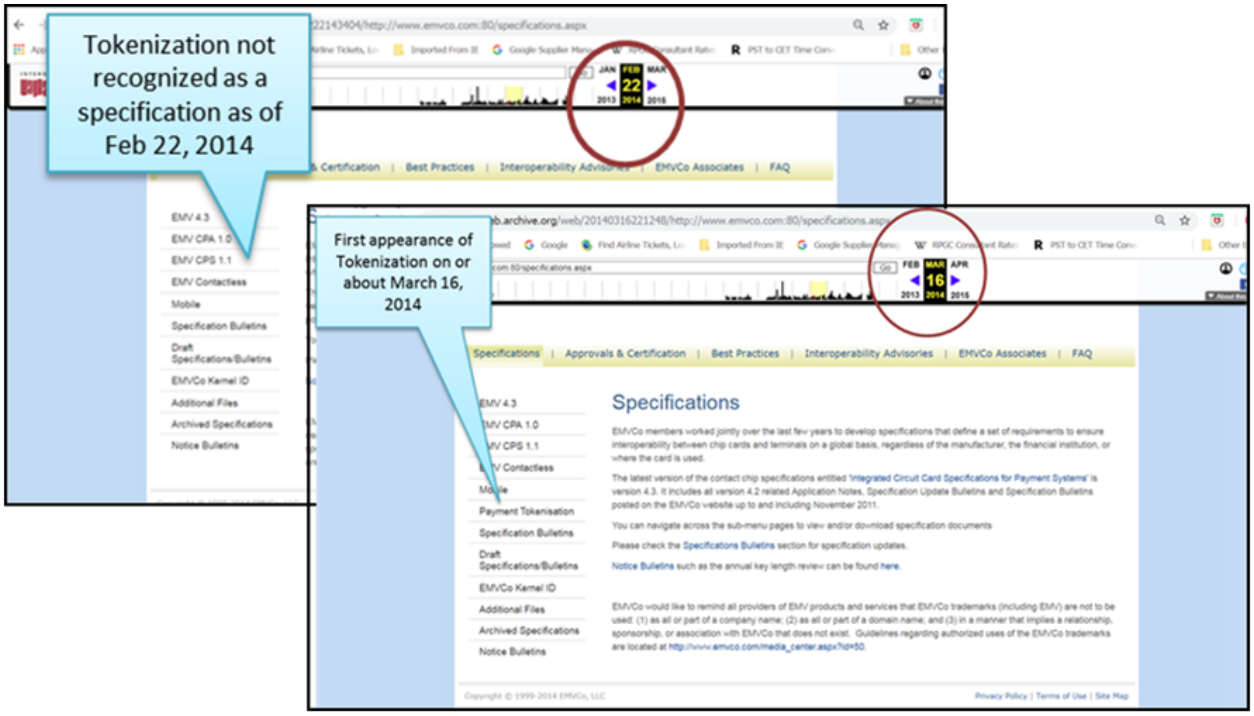

Figure 8 – EMVCo Web Site from February 22 and March 16, 2014 Shows the Sudden Appearance of Tokenization Specification.

* A Bank Identification Number or BIN is the primary account number's (or PAN's) first 6 digits that identifies the issuer of the card and the type of product the card is (e.g. regular consumer credit, Signature Elite, etc.). To protect the card companies' infrastructure, Network Tokens need to look like regular PANs (e.g. 16 digits, start with a "5" or a "4", etc.) so they can be passed around as regular PANs without modifying their systems. Visa and Mastercard allocated special BINs to issue Network Tokens so they can be distinguished from regular PANs but there are a limited number of these BINs, meaning the number of Network Tokens that can be issued is limited. The TSP assigning these tokens are called BIN Controllers

† Fully formed standards have whole numbers (e.g.1.0, 2.0, etc.) Draft specifications have fractional numbers (e.g. 0.8, 0.9, etc.).

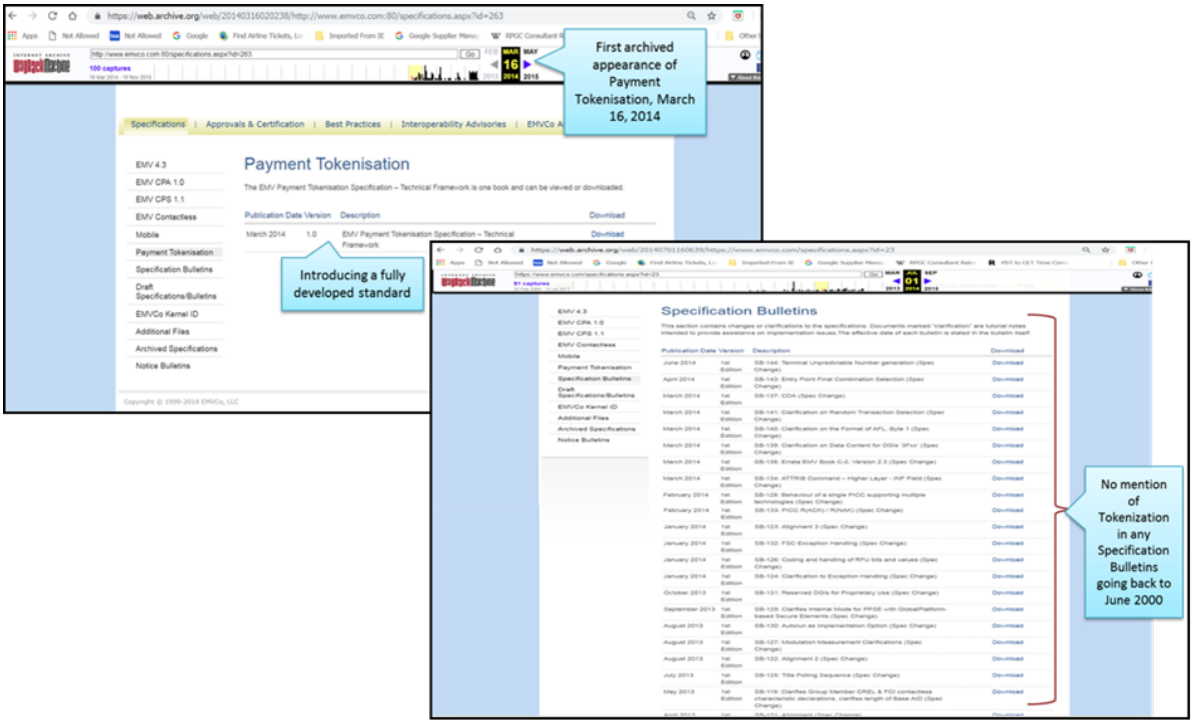

Figure 9 – EMVCo's website shows a lack of bulletins or other development documentation prior to the release of its tokenization standard on March 16, 2014.

9.6 EMVCo Tokenization Framework 1.0 Deficiencies

Industry observers quickly identified major deficiencies in Version 1.0. "Network tokens" introduced friction in customer service and chargeback management environments and created significant challenges for merchants trying to route debit cards through nonaffiliated debit networks.

For example, the use of alternative bank identification numbers or BINs hid useful information from merchants, which is very important to locate orders to address customer service calls as well as to identify chargebacks that could be disputed. More importantly, merchants use BINs to identify the card type as credit versus debit versus pre-paid or business versus consumer, for example, which may determine card acceptance flows. Crucially, BINs are critical to route the transaction through unaffiliated debit networks.

Version 1.0 was based on ISO's older ISO8583 standard for transmitting card data rather than the newer and more flexible ISO20022 standard for financial data in order to maintain compatibility with older systems. This meant that less information about a card and the cardholder could be passed to the issuer. For example, tokens were required to look like cards' 11- to 19-digit account numbers, were assigned from specially designated bank identification numbers used for tokenization and prevent the use of other payment instruments such as bank accounts or private label cards.

Under Version 1.0, there could be multiple tokens for the same primary account number at one merchant. This happened when a cardholder used the same card in multiple smartphones. Version 1.0 did not provide a way for merchants to link these tokens, making it appear as though two different customers were making purchases. Merchants needed to see all these tokens as a single customer so they could provide good customer service, provide loyalty points and manage customer risk.

Finally, it was reported by industry observers that dynamic tokens (a more secure type of tokens that change for each transaction) were excluded from the specification because some large issuers could not support that capability.[39]

9.7 EMVCo Tokenization Framework 2.0 Updates and Remaining Deficiencies

Although promised for late 2014, EMVCo did not complete Version 2.0 until September 2017. Version 2.0 remedied the customer-friction shortcomings of Version 1.0 with the introduction of a "payment account reference" number. Nonetheless, suggestions for mandated sharing of key fields such as type of card, support for ISO20022, inclusion of dynamic tokens and support of other payment methods were all rejected. Crucially, EMVCo also did not address the issue of routing debit cards outside of the card companies' networks, leaving those details to each card company's implementation.

The new payment account reference numbers, also known as PARs, link multiple tokens together for the same customer. A PAR is a 28-digit string that cannot be used to initiate financial transactions, so their sole purpose is to create a single view of a customer's payment channels and methods. Unsatisfactorily, Version 2.0 did not require the card companies to pass the PAR back to merchants. As a result, merchants are more dependent on the networks, potentially having to pay a fee to get PAR numbers.

9.8 Network Tokens Introduce Challenges to Merchant Debit Card Routing Choices

Version 2.0 continued EMVCo's practice of creating obstacles for merchants to exercise their rights to route debit cards through unaffiliated debit networks.

To route debit card transactions from pay wallets such as Apple Pay for in-person transactions through unaffiliated debit networks, the following needs to happen: (1) the bank identification number used to tokenize the debit cards must be registered with the debit networks, (2) the point of sale terminal must be programmed to select the U.S. Common AID (see Section 6) and (3) unaffiliated debit networks must follow rules established by Visa and Mastercard to be able to detokenize a token back to the primary account number or PAN.

These requirements are challenging for merchants for the following reasons: if Visa or MasterCard were to issue a token for a debit card that participates in an unaffiliated debit network but the corresponding token BIN was not enrolled, a merchant would either not route the transaction to the unaffiliated debit network or, if it did, the transaction would be rejected. It is very difficult, if not impossible, to continuously monitor if Visa and MasterCard are issuing tokens that use BINs that may be solely enabled on their networks or hold the card companies accountable for the timeliness of such enrollment with the unaffiliated debit networks.

Further, unaffiliated debit networks can only detokenize transactions that originate using the U.S. common AIDs. Since many terminals have been configured to prioritize Visa and MasterCard global AIDs, a merchant terminal will only select the common AID if it's been configured to ignore the EMV priority. Any merchant that wants to accept mobile wallet-based transactions (e.g. Apple Pay / Google Pay / Samsung Pay) and benefit from the frictionless experience afforded by biometric-only authenticated transactions must chose the global AID rather than the common AID, effectively giving up routing choice.

Once a merchant identifies a debit card token that can be routed through the unaffiliated debit network, the unaffiliated debit network can request that the token be detokenized back to the primary account number. Because the merchant configured the terminal to default to the common AID, however, the transaction is processed as a "no cardholder verification method" transaction. In this scenario, even if the customer uses biometric authentication, the unaffiliated debit network is prohibited from sending that information along to the issuing back. It is important to point out, there are no technical or security challenges with the unaffiliated networks sending this data, it is just an arbitrary card rule. As a result, an issuing bank would consider an unverified transaction as inferior and is more likely to decline it.

Similar obstacles are also found in the card not present environment which includes Internet, mobile commerce and other transactions in which a merchant does not observe a physical card. Visa and Mastercard are actively promoting network tokens to e-commerce and subscription merchants on the basis that their Account Updater service is not

needed.* But while merchants enjoy full routing choice when the primary account number is used, the same is not true of tokenized card-on-file credentials. Mastercard prohibits the routing of such tokenized card-on-file transactions to any other unaffiliated debit networks enabled on the actual card and requires all tokenized transactions run exclusively through their network.

Visa doesn't prohibit the routing of tokenized card-on-file transactions to unaffiliated debit networks, but Visa will only de-tokenize such transactions if the issuer instructs them to do so and will subsequently degrade the service. If a merchant routes the same transaction to an unaffiliated debit network, Visa will detokenize the transaction but will not perform any token domain restriction or cryptogram validation, thereby eliminating the core security capabilities available on such transactions. Because of the perceived lesser security, issuers are more likely to decline these transactions, seriously impacting approval rates and discouraging merchants from routing through unaffiliated debit networks.

Finally, it has been reported by industry observers and representatives of the unaffiliated debit networks that both in the future Visa and MasterCard might require any transaction where the cardholder was authenticated through 3-D Secure on their respective network that the corresponding authorization be processed on their networks. With the push to make adoption of 3DS 2.0 as broad as possible, this will further reduce the number of transactions that can be routed through unaffiliated debit networks.

9.9 EMVCo Failures with Tokenization

With "EMV Payment Tokenization Specification, Tokenization Framework Version 2.0," EMVCo failed to be a "representative of the payments community" in favor of delivering tokenization standards that:

- Are narrowly focused on card companies' products
- Preserve the current infrastructure by using the older ISO8583 communication protocol rather than the more flexible ISO 20022
- Create complexity for merchants and make them even more dependent on services from card companies, with potential new fees
- Are not transparent to merchants, negatively affecting approval and decline rates as well as creating friction for customer service and chargeback departments
- Hide key information such as card type, impacting routing and interchange calculations
- Create obstacles for merchant routing debit of cards through unaffiliated debit networks, in effect providing the card companies with a mechanism to avoid complying with the Durbin Amendment
- Demonstrate, given the difficulty they had evolving the initial tokenization framework to version 2.0, that EMVCo is not the right body to develop these specifications and standards.

Tokenization is one more example of the card companies — specifically Visa, Mastercard and American Express — appropriating an open standard and preempting collaborative industry efforts. EMVCo did not develop the initial tokenization standard at all; the card companies leveraged EMVCo's imprimatur to create the perception that the tokenization framework was an industry standard. In so doing, EMVCo demonstrated, once again, that it creates standards that benefit the card companies at the expense of merchant choice for affordable routing.

* Account Updater is a service offered by Visa, Mastercard and American Express that automatically updates the primary account number and the expiry date of cards-on-file when this information changes. Examples are replacement cards when the card is reissued based on its expiration date. This is an important service for subscription merchants and for merchants that offer cardholders the option to store their cards with merchants for future purchases.

PART III—CONCERNS WITH NEW STANDARDS

This part reviews recently introduced, but not fully implemented standards such as 3-D Secure 2.0 and Secure Remote Commerce that have the potential to significantly disrupt e-commerce and mobile commerce. We will outline concerns with these standards and how they negatively impact the competitiveness of payment solutions in the fastest growing segment of U.S. retail shopping.

10. 3-D SECURE VERSION 2.0

10.1 Background

Three-Domain Secure, also known as 3-D Secure or 3DS, is a security protocol originally developed by Visa. It has been adopted by all the card companies to help prevent fraud when using credit and debit cards to make e-commerce purchases online. It is also the generic name for authentication technology presented to online buyers under the names Verified by Visa, Mastercard Secure Code, SafeKey (American Express), ProtectBuy (Discover), and J/Secure (JCB).

3DS originated with the 2001 Visa Payer Authentication System, which encouraged cardholders to use only Visa cards for online shopping by promoting its exclusive authentication features. That initiative had more to do with brand marketing (with Visa claiming to be secure and others appearing unsafe by comparison) than it did with payment security. Within months, however, the other card companies offered similar solutions. Maintaining multiple authentication standards created logistical problems for merchants, and the card companies acquiesced to a common approach that became 3DS.

The original 3DS scheme, called 3DS Version 1.0, requires that cardholders register with their card issuing banks and that, prior to any e-commerce transaction, they be authenticated by the card issuer. This authentication is performed by redirecting cardholders to issuers where they enter their user-identification and password information. When cardholders are authenticated, the liability for any fraud shifts from the merchant to the issuer.

The initial release of 3DS was not well thought-out and it showed the card companies' inexperience when it came to online shopping. Issuers had little incentive to enroll cardholders because of the liability shift. Aside from the lack of issuer support, online shopping cart abandonment under 3DS 1.0 was high. Many merchants who implemented 3DS 1.0 reported lost sales as customers who were re-directed never returned to complete their purchases, either because they had forgotten their passwords or because the redirection process took too long creating a timeout condition on the merchants' checkout processes.[*]

Despite efforts from Visa and Mastercard to convince online merchants to participate, efforts that included meaningful financial incentives, adoption remained low due to increased friction and lost sales.[†] More importantly, 3DS 1.0 lacked support for card-on-file and recurring payments, important payment modes for online shopping and subscription merchants. Thus, what is now called 3DS 1.0 was poorly designed, mismanaged in its implementation and was minimally adopted by U.S. merchants.

10.2 Evolution from 3DS 1.0 to 2.0

Like tokenization, 3DS was not developed by EMVCo. Its implementation as a standard is another case of the card companies using EMVCo to bolster technologies that structurally support their objectives. 3DS was "re-invented" by the card

[*] A "timeout" is the cancellation of an order that automatically occurs when a predefined interval of time has passed without a certain event occurring such as getting a response from a provider

[†] Visa offered merchants large cash or marketing rebates, sometimes in the multi-million-dollar range. Mastercard introduced interchange reduction on 3DS transactions in addition to the liability shift.

companies during 2013-2014 because of separate compounding circumstances:

- Increases in online fraud rates led issuers to tighten their risk scores and to decline authorization requests at higher rates. For this reason, merchants and issuers, dissatisfied with the card companies' solutions to the problem, decided to explore ways for merchants to share richer information with issuers, potentially using third party solutions that would pass this information outside the card companies' control
- The emergence of competing authentication standards from the FIDO Alliance and W3C
- The impending arrival of European Commission's Payment Services Directive 2, which required "strong customer authentication" on all online transactions.*

These events led the card companies to rethink how online transactions are authorized and how they could avoid being disintermediated by creating an authentication standard.

10.3 3DS 2.0 Pre-empting Competition

To increase approval rates, large merchants such as Microsoft, Google and Netflix reached out to selected issuers around 2013 to explore "out of band" solutions. Both merchants and issuers concluded that approval rates could be improved if better data were available during the issuer's decision-making process. Additional data discussed included information such as email address, IP address, device fingerprint and length of relationship between the cardholder and merchant.

Unfortunately, the card companies and many issuers were, and still are, running their authorization platforms on the ISO8583 message format standard, which, although very robust, is not very flexible. ISO8583 does not have the capability to carry the additional information issuers wanted. Issuers realized that they were missing out on interchange income due to unnecessarily declined transactions and began cooperating with merchants in exploring solutions that bypassed the card companies. Some innovative financial technology companies offered "out of band" messages running parallel to the authorization flow, which conveys the data to the issuer. Companies such as Ethoca and Cardinal Commerce, for example, were well-positioned to provide such services.

Faced with these issues, Mastercard announced in November 2014 that it would join Visa in creating a new version of 3DS that would carry richer data, a move that preempted the work of other companies.† In January 2015, EMVCo owners agreed that the draft framework and corresponding intellectual property developed by Visa and Mastercard would be handed off to EMVCo for further development. Although promised for late 2015, it was not until October 2016 that EMVCo published its standard for 3-D Secure 2.0, which could deliver much of the data sought by issuers to increase approval rates.

10.4 3DS 2.0 Positioned as a Strong Customer Authentication Standard

On November 16, 2015, the European Commission enacted Payments Security Directive 2, which extended changes originally implemented in 2009.‡ Under PSD2, financial institutions were mandated to open access to bank accounts to any qualified payment initiation service providers. In order to protect consumers, PSD2 also required —with some exceptions — that account access must be done with strong customer authentication, which is generally referred as SCA, a methodology to authenticate the

* The EU Committee released its PSD2 proposal in 2013 and was finally adopted in 2015.

† This risk of disintermediation is no longer the case after Visa's acquisition of Cardinal Commerce in 2016 and Mastercard's acquisition of Ethoca in 2019.

‡ The original PSD regulation opened the payment markets to payment service providers who were not financial institutions. Payment Service Directive 2 is officially known as Directive (EU) 2015/2366 amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

account owner based on multi-factor authentication.[*]

The requirement applies to all remote payment transactions initiated by a payer within the European Economic Area, including card transactions, but applies only on a "best-effort" basis when one of the parties is located outside of Europe. Exemptions are also allowed for low-value and recurring transactions.[†] However, it is believed that U.S. merchants selling in Europe that do not perform strong customer authentication could see significant loss of sales as European card issuers expect this authentication to be performed regardless of the "best-effort" exclusion.

Visa and Mastercard immediately positioned EMVCo's new standard, 3DS 2.0, as the best tool to perform strong customer authentication for card transactions both in Europe and the United States.[‡] The decision is another example of EMVCo standards being developed and leveraged in a way that benefits the card companies' existing practices while increasing merchants' payment processing costs and inhibiting true security innovation.[§]

10.5 EMVCo Ignores Authentication Standards from Other Standards-Setting Bodies

EMVCo's traditional area of expertise has been chip cards and terminals, not biometric technologies nor consumer authentication. By contrast, the FIDO Alliance has been developing alternative authentication approaches for several years. Similarly, the Web Payments Working Group of the World Wide Web Consortium (W3C) initiated work on its Payment Request application programming interface with participation from a cross-section of industry stakeholders intended to create the concept of "payment apps."

In collaboration with the FIDO Alliance, W3C advanced the Web Authentication API, named WebAuthn and in March 2019, WebAuthn became an official web standard. WebAuthn, is supported in Windows 10 and Android and it is being implemented in Chrome, Firefox, Edge and Safari. WebAuthn addresses some of the risk analysis goals of 3DS 2.0 through new browser capabilities that enhance user privacy.

Payment apps like WebAuthn are intended to standardize the buying experience and run on desktops, laptops, tablets and phones. They provide services such as strong user authentication, loyalty program integration, and back-channel communications with the merchant for fraud analytics. More importantly, WebAuthn is designed to "support the broadest possible array of payment methods." Yet none of these approaches to customer authentication have found their way into the card companies' initiatives for safer payments in the United States.

Instead of collaborating with open standards-setting organizations, EMVCo pursued expanding the 3-DS-based framework developed by Visa and Mastercard. In so doing, the card companies retained control of the authentication process and prevented other payment methods from participating in it.[**]

---

[*] PSD2 regulations define strong customer authentication, or SCA, as an authentication based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent and that protect[s] the confidentiality of the authentication data. The regulation was originally schedule to be effective on September, 2019 but due to the lack of industry readiness, the effective date for the application of this regulation has been moved to the last day of December, 2020

[†] The Regulatory Technical Standards or RTS provides detailed specifications to achieve the strict security requirements for payment service providers in the EU.

[‡] Even though neither PSD2 nor RTS mention 3DS, many merchants believe that PSD2 have mandated 3DS, failing to recognize that 3DS is just one alternative to comply with the SCA requirement.

[§] Mastercard charges a $0.03 for each Secure Code verification attempt and acquirers planning to offer SCA are quoting charges from $0.02 to $0.07 per 3DS 2.0 verification on top of that.

[**] EMVCo collaborates with open standards-setting organizations but only when it benefits their owners. In one example, EMVCo provided payment use cases to the FIDO Alliance for incorporation into its Authentication Suite. Doing so allows FIDO certified authenticators such as fingerprints and facial recognition to authenticate card transactions. By working with W3C and the FIDO Alliance, EMVCo can claim that they collaborated in payment technology. In the end, providing these use cases had the desired optics: In its related press release, the FIDO Alliance unfortunately mislabels EMVCo "the global payment standards body," continuing to foster the image that EMVCo speaks for the entire payments industry.

10.6 Industry Concerns with 3DS 2.0

3DS 2.0 is a new standard that has not been widely deployed by vendors or adopted by merchants. Much of the recent impetus for its implementation was driven by the European strong customer authentication requirements.[*] Because it is still early days, there are few 3DS 2.0 practical experiences to study its impact on the U.S. payments industry. However, observers have identified issues and expressed concerns regarding this standard that echoes problems noted with other EMVCo standards.

- The architecture of 3DS 2.0 is essentially similar to 1.0 – a 3DS server connecting to a directory server which, in turn, connects to an issuer's access control service. Given that the amount of data being passed is greater, there are significant concerns about performance and the possibility of cart abandonment because of timeout conditions. This was a big problem under 3DS 1.0 and reports from a recent EMVCo meeting indicate that the 3DS 2.0 authentication roundtrip suffers the same performance issues.
- 3DS 1.0 had little adoption amongst U.S. merchants because of the friction it introduced in the shopping process but, at least, merchants had the option to use 3DS 1.0 or not. There are concerns within the merchant community that the card companies will mandate 3DS 2.0. Under EMVCo's secure remote commerce, also known as SRC but branded as "Click to Pay", merchants lose control over whether 3DS 2.0 is executed as the authentication process is now being performed by the wallet operating under SRC.[†]
- Another major concern about EMVCo's 3DS 2.0 standard is that it lets the card companies define rules that prevent routing of debit cards through unaffiliated debit networks. Unconfirmed reports from merchants and other industry sources indicate that Mastercard will require all 3DS 2.0 authenticated transactions to also be authorized and settled through their network instead of the unaffiliated debit networks, violating the spirit and the letter of the Durbin Amendment.
- The card companies continue to position the EMVCo 3DS 2.0 standard as the tool to address the European requirement for strong customer authentication, pushing merchants to implement it even though there are also concerns, voiced by the European Banking Authority that, under certain conditions, 3DS 2.0 does not meet their authentication requirements.[‡] Thus, merchants are concerned about implementing 3DS 2.0 but still not being compliant. A companion concern from industry observers is that, by putting all the attention on EMVCo's 3DS 2.0 standard, other authentication approaches from competing companies or open standards bodies are being pre-empted.
- Conveniently, EMVCo's definition of the 3DS 2.0 standard allows the card companies to define fees and other governance rules. The card companies have historically taken advantage of these opportunities to introduce additional merchant fees. For example, when tokenization was introduced in 2013, Mastercard began assessing a 0.01 percent Digital Enablement Fee which applies to all online transactions – e-commerce and mobile commerce - even if the merchant does not use Mastercard's tokenization services. Similarly, since approximately 2013 Mastercard has also been charging a Secure Code transaction fee of $0.03 for every 3DS 1.0 verification attempts. Given this precedent, it is reasonable to be concerned about the

[*] Strong Customer Authentication was scheduled to go live in September 2019 but has been delayed until the last day of 2020

[†] This will be discussed at length in the next section on secure remote commerce

[‡] 3DS 2.0 without biometric authentication cannot be used to satisfy the inherence factor requirement under strong customer authentication, just knowledge and possession.

possibility of the card companies introducing or raising 3DS 2.0 fees.

10.7 Conclusion

While EMVCo did not develop the original 3DS standard, its assumption of the standard was critical to its credibility. 3DS 2.0 follows the pattern of the card companies preempting industry efforts and creating barriers to market entry for better payment methods as well as creating standards that introduce fee-generating services. 3DS 2.0 shows, once again, that EMVCo acts as a pass-through company to create standards that benefit the card companies, not the overall payments industry.

12. SECURE REMOTE COMMERCE

12.1 Background

Secure Remote Commerce is a recently introduced EMVCo standard intended to provide a unified checkout for remote commerce where purchases are done via web browsers or mobile phones and where the physical payment card is not present. To users, SRC will appears as a single button with a variety of payment methods from the card companies that are enrolled in the SRC system the merchant has implemented.

The document that defines the SRC standard is a technical framework draft released in March 2017 that broadly described its concepts, including the roles and responsibilities to be held by the different participants in the SRC system. Early merchant implementations of SRC began to appear in October 2019 under the name "Click to Pay" but the card companies do not expect major adoption until after the 2019 holiday season.[40]

The SRC standard creates a new checkout experience while enabling integration with other EMVCo standards such as 3D Secure and tokenization with the objective of delivering to merchants an experience similar to the point of sale: receipt of a payment token that the merchant can use to initiate a secure remote payment.

EMVCo has stated that the objectives of the EMV SRC standards are to:

- Design uniform interfaces that allow for secure exchanges of payment data among participants in the digital commerce environment
- Accommodate options for using dynamic data — such as cryptograms or other transaction-unique data — to enhance the security of payment transactions on a merchant's SRC-enabled website, mobile app or other e-commerce platform
- Enable compatibility with other EMVCo technologies such as payment tokenization and 3-D Secure
- Facilitate consumer recognition of a common user experience by display of the SRC icon

EMVCo states that today's e-commerce environment "…has many different integration models and practices. The variety of implementations and the lack of common specifications for this environment results in fragmentation, complexity and inconsistency."[41] EMVCo purports to address the need for consolidation, simplicity and interoperability by providing a "universal buy button" that contains cardholder payment information which can be used at all SRC-enabled merchants.

The card companies claim that their motivation for introducing this standard is to simplify the checkout process and eliminate the confusion created by the large number of checkout buttons. Ironically, the proliferation of checkout buttons was caused by the card companies themselves trying to compete with other user-friendly and secure solutions such as PayPal. Since the card companies have failed to gain much market adoption, SRC seems to be an attempt to rewrite the checkout button display rules. EMVCo's SRC is a solution in search of a problem—unless one concedes that the problem is branding and increased market share for EMVCo's owners.

12.2 Game of Buttons

The card companies care about both their brands and about transaction volume; one is critical to maintaining the other. That is why, for example, Visa and Mastercard lament that consumers often say they are "paying with PayPal" when the actual funding instruments are their credit or debit cards linked to consumers' PayPal accounts. It was not surprising that when PayPal grew out if its eBay origins around 2006, the card companies became concerned that it would be considered a competing "acceptance brand".

Prior to 2006, the card companies had very strict rules regarding the display of their logos on websites. All logos had to be displayed equally and there could

not be a preference between logos. The card companies were so concerned that they required that the PayPal logo on merchant sites comply with their regulations with regards to size, color and other considerations as a "comparable" logo. A pre-2006 merchant checkout logo display looked like that shown in Figure 10.

Figure 10 — Checkout logos prior to 2007

Figure 11—Logos from 2007-2009 featuring "Check out with PayPal

Around 2007-2008, however, PayPal found a way to achieve prominence by convincing merchants to implement a larger button that initiated a new "process" running in parallel to the process of card-based checkouts. "Check out with PayPal" gave PayPal greater visibility, as shown in Figure 11.

Despite the negative reaction and threats from the card companies, PayPal was able to prevail because it argued that this approach did not violate the rules, as "Check out with PayPal" was not a comparable product but a different "process." PayPal created multiple versions of its "buy buttons." Some merchants even presented the "Check out with PayPal" button alongside plain text saying "check out with credit cards" that did not show any of the card companies' logos.

Around 2011-2013, the card companies tried to compete with PayPal at its own game by developing their own checkout buttons. Visa introduced V.me in 2011 which evolved into Visa Checkout; Mastercard introduced PayPass Wallet Services in 2012 which evolved into Masterpass and Amex Express Checkout was introduced in 2015. Each of these buttons appeared with varying degrees of marketing fanfare but they all had low customer and merchant adoption. Their functionality was still rudimentary and comparable with what PayPal had offered in 2002. Still, the card companies persisted, leading to the proliferation of buttons — as shown below — that EMVCo now claims is causing consumer confusion and creating a reason to introduce SRC (see Figure 12).

The card companies' concerns are not just about brand prominence. E-commerce provides a real opportunity for new, competing payment methods to be introduced. Consumers are more likely to adopt new online payment forms while the infrastructure cost for merchants to implement them is a fraction of the cost associated with adopting new forms of payment in-store. EMVCo consolidates the resources of the card companies against services like PayPal and interferes with efforts of other standard bodies before they can gain momentum.

Shortly after EMVCo's announcement of the Secure Remote Commerce initiative in late 2017, the card schemes—led by Visa, Mastercard, and American Express—launched public relations efforts to

Figure 12—Logos in checkout page circa 2015 cluttering the checkout page with a button for each major brand

buttress EMVCo and SRC which left no doubt as to who their target was (see Figure 13 below): wallets not associated with the card companies' checkout buttons.*

Similarly, the World Wide Web Consortium, known as W3C, launched its Web Payments Initiative in 2014. Its stated objective was to enable consumers to choose their preferred payment options across all

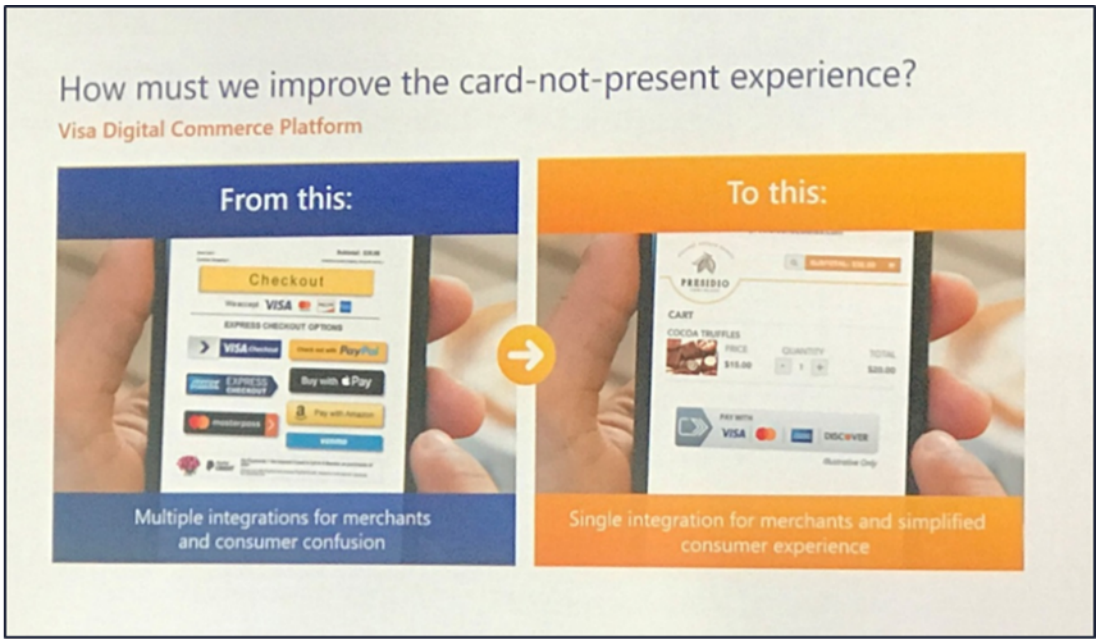

*Figure 13—Slide from a Visa presentation showing replacement of all competing checkout logos with a single SRC logo**

One of SRC's functions is to authenticate cardholders before adding their payment cards to the SRC wallets. In the early implementations, this authentication is being performed via one-time codes sent to the e-mail address or mobile phone registered with the card. This approach ignores the ongoing authentication work of the FIDO Alliance and W3C.

For example, the FIDO Alliance's open standards-making process, started in 2013, encouraged and invited participation from all companies and organizations that wanted simpler and stronger online payment authentication. Participation in FIDO, in contrast with EMVCo, is open to any paying member and includes voting in board meetings. FIDO Alliance's objective is to define an open system that benefits *all* users of the internet.

their devices, for merchants to transparently support a growing number of payment options, for new payment providers to enter the market more easily with innovative solutions and payment systems, and to support new payment models such as micropayments and payment wallets. W3C's standards development process is fully inclusive and transparent. From its launch, W3C's initiative was open to participation from all the members of the payment community.† The initiative speaks directly about preventing vendor monopolies and includes all forms of payment, including ACH and non-traditional payment methods.

Rather than pursuing similarly open systems, EMVCo states that "EMV SRC is focused on providing consistency and security for **card-based payments** [emphasis added] within remote payment environments" and that "EMVCo aims to work

* Picture from a presentation by Alfred Kelly, Visa CEO at JP Morgan Global Technology and Communications Conference, Boston, May 2018

† To see the inclusiveness of W3C participating members, see https://www.w3.org/Payments/WG/charter-201803.html

closely with industry participants such as W3C to capitalise on opportunities for alignment where appropriate."[42]

In a June 2018 EMVCo ad-hoc meeting in San Diego to discuss SRC, EMVCo stated that its inability to work with W3C was due to intellectual property issues because W3C and EMVCo work under different confidentiality models. W3C's working groups operate in public, so if a group reviewed an EMVCo standard it would have to release those findings publicly, which EMVCo would not allow as it operates behind closed doors. EMVCo's opposition to transparency in the standard setting process is, in fact, the problem itself. At the same meeting, attendees criticized EMVCo's inability to define specific roles and processes for participation by any competitors to the card companies in the SRC programs.

It was not until April 2019 that EMVCo joined the FIDO Alliance and W3C in creating a new interest group to collaborate on a vision for web payment security and interoperability. In its press release, EMVCo said it looked forward to "productive discussions and ultimately increased interoperability for payments."[43] It remains to be seen what develops from this interest group, given EMVCo's history of superseding other standards-setting bodies' work and operating in a closed-door environment.

12.3 SRC User Experience

The initial SRC implementation at merchants' checkout pages shows a process very similar to what consumers do when they create PayPal accounts (the numbers detail the windows in Figure 14 below):

1. In merchants' pay page consumers click on the Click to Pay button. This brings up a widget or java script window where consumers enter their e-mail address to register or login. The widget or java script is hosted by the company or SRC program with whom merchants entered into an agreement with, either Visa or Mastercard. In the example below, the widget presented is by Visa.
2. The window asks for payment card information from new consumers. Note that the window only allows entry of 15 to 16-digit payment card numbers (rather than bank or other account number) and that once the card number is determined to be a Mastercard, the host of the window changes to Mastercard.
3. Consumers must provide additional information such as billing address which is also used as the default shipping address. This process is similar to enrollment in any other e-wallet enrollment.
4. The SRC program sends a one-time use code to the email address of record for that payment card. It is not known at this time whether this process uses the 3-D Secure or another proprietary protocol. The e-mail

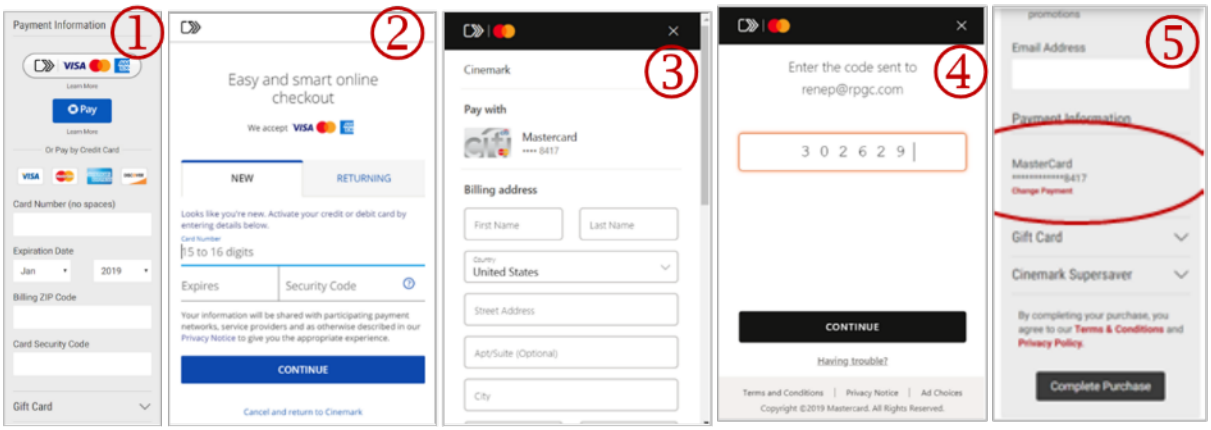

Figure 14—SRC user experience

comes from Visa or Mastercard, depending on the card type, not from the issuer.

5. Once the number is entered and verified, a token is passed back to the merchants who can either use it to initiate the payment or store it for future use. The actual primary account number may or may not be passed to the merchant depending on SRC program's implementation rules. The primary account number is optionally tokenized and bound to the device that initiated the transaction by means of an algorithm that indicates the token associated with the primary account number can only originate from that device.

In subsequent SRC experiences – either with the same merchant or any other merchant, consumers do not have to re-enter their primary account number or credentials as the card number is already registered and bound to the device in question. Consumers enter their e-mail addresses and the one-time code on the widget or java script window which will cause the SRC programs to pass the payment data to the merchant. Optionally, consumers can set their phones or computers as trusted devices and this will prevent the need to enter the one-time code when they do subsequent purchases.

12.4 EMVCo SRC Standard Components

The unprecedented collaboration between the card companies and EMVCo has delivered a complex standard with many participants and roles:

- SRC program: Responsible for the policies and processes associated with the oversight of SRC participants within an SRC system. This role is expected to be performed by the card companies.
- SRC system: Orchestrates all activities between participants and manages technical aspects of the SRC program. This role is also fulfilled by the card companies.
- Digital shopping application: A payment application (on the merchant side) driving the consumer experience for SRC. This function can be provided by the merchant or a payment service provider.
- SRC initiator: Supports checkout and/or the secure retrieval of payment data from the SRC system on behalf of a digital shopping application. This is provided by merchants or their payment service providers.
- SRC participating issuer: Issuers who decide whether to enroll their payment cards with a given SRC system.
- Digital card facilitator: Holds payment card data and makes it available to support the checkout process. The role is rather open and, while card companies' payment wallets — such as the replacements for Masterpass and Visa Checkout — could fulfil this role, the question is whether the role is open to any other participants and, if so, under what conditions.

Understanding these roles is important because rules and regulations for these programs flow from the top. Both Visa and Mastercard have introduced SRC programs but few details have been published publicly about their implementation, especially about rules and fees.

12.5 Issues with the Development of SRC Standard

The history of SRC reveals a pattern of the card companies trying to create a card-biased future for remote payments. The EMVCo SRC standard was developed in a closed collaboration between the card companies that own EMVCo, primarily Visa, Mastercard and American Express. Early versions of the SRC standard were developed with little influence outside of the card companies but, given the continued volume growth in the web and mobile commerce channels, industry stakeholders clamored for the opportunity to provide input.[*]

[*] In 2017, consumers spent $453.46 billion on the web for retail purchases, a 16.0% increase over 2016. Overall, e-commerce accounted for 49% of the growth seen in retail in 2017. https://www.paymentscardsandmobile.com/major-card-schemes-set-for-simpler-e-commerce-via-emvcos-secure-remote-commerce/

After considerable pressure, and in an unprecedented move, EMVCo released a draft standard – "Version 0.9" – for public comment in the fourth quarter of 2018. However, the public was given only forty-five days to review 329 pages of technical content with no context beyond the published 30-page high level framework. Despite request for clarification and for opening of the standard from the broader market, little changed from the draft standard when the final Version 1.0 was published in June 2019. In a prime example of its flawed structure, EMVCo purports to allow others the opportunity to be heard, and "have a voice" but, in the end, no one outside the core owners can really influence outcomes. Shortly thereafter the card companies announced their plans to launch Secure Remote Commerce programs during the latter part of 2019. Based on the timing of these announcements and the publication date of the final Version 1.0, the card company product plans were likely developed based on a draft specification prior to public input.

Despite EMVCo's claims of incorporating extensive industry feedback during this review process, sources interviewed for this paper (who wished to remain anonymous because of the nonpublic nature of their discussions) reported having been left with many unanswered questions about the participation of U.S. unaffiliated debit networks and the ability of merchants to route transactions to the networks of their choice. Participants also reported questions about key roles and responsibilities that were delegated to the card companies.

12.6 Industry Concerns with SRC Standard

EMVCo leaves many SRC operational implementation choices to the sole discretion of the card companies. Although the use of 3-D Secure and tokenization are optional, there are major concerns that choice and routing limitations experienced with other EMVCo standards will be replicated within SRC. EMVCo states that use of non-EMV tokens and routing decisions are outside the scope of the SRC standard and leaves those decisions to the card companies, potentially limiting the choice of products or solutions that support enhanced security and competitive choice for merchant routing.

The rules and regulations for SRC programs are proprietary to the card companies. EMVCo has chosen to defer to its member owners in strategic areas where the companies can leverage their market strength to create entry barriers for competitors. SRC threatens PayPal, Alipay, Google Pay and Amazon Pay by potentially limiting their participation in SRC programs. Such reduction in competition would also affect merchants' and consumers' choices.

Merchants are also concerned that they might not be able to incorporate or prioritize their own proprietary payment products within SRC digital card facilitators. Despite feedback provided during the draft specification public comment period, the initial Version 1.0 specification does not allow a merchant or consumer to prioritize the payment cards within the candidate list presented to the consumer within SRC checkout on a merchant's own website. Mastercard has subsequently pushed EMVCo to modify the standard to enable prioritization within the candidate list of its co-branded cards. However, the optimal solution calls for merchant and consumer choice of that prioritization for all cards within and outside of SRC.

Based on SRC program hierarchy, a high-level review of both the SRC framework and draft standard as well as review of the early SRC implementations, we identify potential outcomes that could negatively impact other payment industry stakeholders:

- In theory, merchants can create their own proprietary SRC programs. However, both networks have communicated that existing wallets, such as the reincarnated Visa Checkout and Masterpass, will be the first ones to transition consumers to SRC. Both Visa and Mastercard have been able to launch their SRC programs in October of 2019 due their "inside" view into the development of the standard through EMVCo. Neither EMVCo, Visa or Mastercard have published their implementation guides for merchants at large to consider the effort, investment, or opportunity of taking this step.

- Early merchant implementations show the digital card facilitator or wallets to be a re-incarnation of Visa Checkout and Masterpass. There can be multiple digital card facilitators connected to one SRC program, but it is the SRC program that determines the facilitator selection criteria.[*44] These criteria are not defined in the standard and are left to the discretion of the SRC program owners. Will the card companies, in their roles as SRC program owners, limit or deprioritize facilitators other than their own, limiting competition?
- All the account information stored in digital card facilitators is card-based and does not provide for any other type of account. Payment card data as defined in the standard is an 11- to 19-digit account number generated within ranges associated with a bank identification number by a card issuer.[†] This automatically limits payment instruments to cards, preventing any competing payment methods from participating.
- The EMVCo standard leaves to the discretion of the SRC programs whether to share payment data beyond the token, expiry date, and other relevant information required to process a payment. Merchants are concerned that the card companies may choose not to share other important information such as the primary account number, bank identification number or card product type, all important elements for merchants to decide their routing and processing options.
- The EMVCo standard offers choices with regards to the level of security enabled, which suggests security is dependent on the SRC implementation. For example, device binding may not be implemented in the initial market deployment by one SRC system while another SRC system may choose to enable device binding upon the initial market deployment. An open payment standards body should be setting standards that meet minimum security requirements based on collective aggregate input from all stakeholders versus leaving those decisions to the card companies, which are the early implementors.
- The implementation by each SRC program imposes costs, rules and requirements that are set by the card companies. This creates a large concern for merchants as to what SRC will do to their total cost of payments: Will there be a fee for associating third-party digital card facilitators to an individual SRC program? Will there be a digital card facilitator fee to resolve a request for payment data to the merchant or to provide additional payment data? Will Visa and Mastercard also assess additional fees for their tokenization services, as was originally suggested when the Visa Token Service and Mastercard Digital Enablement Service were introduced? Will Visa and Mastercard, the two initial SRC program owners, charge an additional fee for processing transactions through their SRC systems?

Finally, although merchants' acceptance of SRC has been communicated initially as a choice, it is concerning that card companies could, in the future, mandate merchants' participation under their proprietary rules. Smaller merchants may not have a choice of SRC participation as they are heavily dependent on their payment service providers. In addition, the card companies may use financial penalties or incentives to force merchant adoption of SRC and restrict competition on merchants' checkout pages.[‡]

[*] The SRC Program establishes proprietary criteria that defines the selection of a specific Digital Card Facilitator

[†] Although the standard specifies 11 to 19 digits, the early implementations of SRC by Visa and Mastercard under the banner "Click to Pay", limits the types of forms of payments even further by only allowing account numbers of 15-16 digits in length

[‡] There is a precedent for this behavior. In the early 1990's Visa established the electronic interchange reimbursement fee, also known as EIRF, to incent merchants to adopt electronic authorization rather than continue using floor limits. It is, therefore, reasonable to be concerned that the card companies could price non-SRC transactions at a higher interchange.

12.7 Conclusion

In theory, some of the ideas behind SRC are good: lowering fraud while enhancing consumers' experiences are hard to argue against. Complaints are not with the concept behind SRC, but with the development of this standard without meaningful public input. EMVCo claims standardization and interoperability justify SRC's existence, but EMVCo is a closed environment providing prioritized benefit to its owners. At this time there is no indication that SRC will be interoperable with unaffiliated debit networks or any other competing system, other than general oral representations at public forums that "nothing will change" with regards to processes behind the button. If history is an indicator, SRC will be restricted to the card companies' brands and products, just as all other EMVCo's standards have restricted competitive products and services.

EMVCo claims that it "has the strategic breadth, industry knowledge and technical ability, coupled with a proven record of specification delivery, to facilitate the development of secure and interoperable remote payment solutions ... that maintain compatibility with the existing payment infrastructure."[45] What is clearly missing from this list is an open and inclusive environment for all stakeholders to participate and affect outcomes.

With SRC, the card companies are leveraging EMVCo standards in a bid to limit competition in online commerce. Cards are losing market share to alternative payment methods, and their own Visa Checkout and Masterpass were dismal failures. The card companies' concern for e-commerce customer experience is a veil for revitalizing card-brand dominance in online commerce. Merchant and consumer groups are justified in their growing skepticism about SRC even as the card brands continue to increase their drumbeats for premature adoption that preempts both present and future competition.

PART IV—CONCLUSIONS

13. CONCLUSIONS

The questions asked in the beginning of this paper were:

- Is EMVCo furthering the entire U.S. payments industry or simply protecting Visa and Mastercard's market share?
- Is EMVCo capable of developing standards in areas beyond its original charter and are these standards delivering more efficient and secure payments?
- Is the U.S. payments industry's competitive landscape being hurt by allowing EMVCo to establish broad payment standards and should this work be performed by true open standards-setting bodies?

13.1 Is EMVCo Protecting Visa's and Mastercard's Market Share?

Yes. EMVCo is a vehicle for collusion among the card companies on payment standards. Visa and Mastercard use this process to jointly work on technology and processes that benefit them, preserving or increasing their market dominance, while stifling the emergence of any competition. The card companies hand their work to EMVCo, which turns it into standards, giving the patina of credibility to technology that is biased in favor of the card companies. Despite claiming to only create "specifications," EMVCo produces standards implemented in a near-identical manner by the card companies and, when EMVCo releases standards, the card companies are immediately ready to implement them because the card companies *are* EMVCo and they design the standards to meet their needs.

Visa's and Mastercard's obfuscation efforts to create the impression that EMVCo is an independent organization are unconvincing. EMVCo's Board of Managers is made up exclusively of long-term card company employees, none having less than 10 years' tenure. These individuals' function without any checks from other sectors of the U.S. payments industry such as bankers, merchants or consumers to counterbalance their perspective.

EMVCo operates in opacity and with no accountability to anyone but its owners. The input provided by its technical and business associate members is limited almost entirely to card payment processing companies that need to understand the impact of the new standards to their own platforms. Because all decision-making powers are limited to only EMVCo's owners, merchants recognize that joining EMVCo is not effective and are underrepresented.

EMVCo claims to be the representative of the global payments industry. This paper concludes that EMVCo is not an appropriate standards body and does not represent the industry. True standards are developed in a collaborative manner in open forums with diverse and inclusive representation of all stakeholders. That is not the case with EMVCo which is structured to deliver standards that benefit only the card companies and protect their market share.

13.2 Is EMVCo Capable of Developing Standards in Areas Beyond its Original Charter?

No. Throughout its history, EMVCo has sacrificed payment security for the convenience of the card companies and for retaining or increasing those companies' transaction volume. Its standards constantly limit merchant choice for transaction routing, in violation of U.S. federal law. This paper concludes that:

- EMVCo betrayed its own charter to provide secure chip card payments by acquiescing to, and ultimately supporting, Visa's 20-year-plus battle against U.S. PIN-based networks and Visa's insistence on chip and signature instead of PIN.
- EMVCo introduced a complex, expensive and unwieldy system for mobile payments using near-field communication technology

because it protects the status quo of its owners while preempting the work of other standard-setting organizations and preventing competitors entering mobile payments;

- EMVCo co-opted tokenization standards work from other organizations and developed an anticompetitive tokenization standard that discriminates against debit networks and non-card forms of payment.
- EMVCo ignored the work of the FIDO Alliance and W3C regarding open standards for authentication that would have also been available to non-card payment systems, instead adapting the card companies' 3DS system to preempt the market from competitive solutions.
- EMVCo is now preempting the market and coopting standards for e-commerce by asserting itself as the "representatives of the payments community" to develop a Secure Remote Commerce standard that will make it difficult to route transactions through unaffiliated debit networks, create higher dependence on the card companies and increase merchants' payment processing costs.

13.3 Is the U.S. Payments Industry's Competitive Landscape Being Hurt by Allowing EMVCo to Set Standards?

Yes, the United States lags many countries when it comes to payments. QR code-based mobile payments are the norm in many Asian countries, for example, while tap-and-go- contactless payments have been widely adopted in the United Kingdom, Canada and Australia, and both UK and European consumers have access to real-time bank transfers. Consumers in these countries have more options to pay that are convenient to them whereas merchants also benefit as competition keeps lower payment costs lower than what U.S. merchants pay.

Meanwhile, the card companies — primarily Visa and Mastercard – use EMVCo as their surrogate as they seek to foster an archaic, card-based environment that is one of the most expensive and fraud-prone systems in the world. EMVCo missed the mark in selecting NFC instead of opening mobile payments to other technologies such as QR codes and stifled new possible payment systems by implementing a narrow tokenization standard that does cannot accommodate other payment methods.

While EMVCo claims to promote "compatibility" and "interoperability" in order to provide "secure" transactions, those are code words for control and preservation of the status quo for card companies. EMVCo standards exclude other forms of payment and create barriers to merchant choice in a way that is continuous and stifling. EMVCo's de facto standards cause all payment industry participants – including merchants, card-issuing banks and merchants' "acquiring" banks – to spend millions of dollars on implementation. Doing so all but eliminates the possibility of investing in alternative payment methods.

It is our conclusion that the U.S. payments industry is being harmed by the card companies and EMVCo. The setting of payment standards for topics such as authentication and tokenization should be migrated away from EMVCo to independent and neutral national or international standards-setting bodies. EMVCo's collusion with the credit card companies has put profits ahead of security, driven up costs for businesses and consumers alike, and has left the United States with a fraud-prone payment card system even as fraud has been reduced in the rest of the world.

PART V—ENDNOTES

[1] "A Guide to EMV Chip Technology Version 3.0," EMVCo, December 18, 2017, https://www.emvco.com/terms-of-use/?u=wp-content/uploads/documents/A-Guide-to-EMV-Chip-Technology-v3.0-1.pdf.

[2] Claire Greene and Joanna Stavins, "The 2017 Diary of Consumer Payments Choice," *Diary of Consumer Payments Choice by the Federal Reserve Bank of Atlanta* no. 18-5 (2018), https://www.frbatlanta.org/banking-and-payments/consumer-payments/research-data-reports/2018/the-2017-diary-of-consumer-payment-choice.aspx.

[3] "The Federal Reserve Payments Study: 2018 Annual Supplement," the Federal Reserve System, December 2018, https://www.federalreserve.gov/newsevents/pressreleases/files/2018-payment-systems-study-annual-supplement-20181220.pdf.

[4] Jim Daly, "Interlink Starts Growing Again And Visa Prospers Despite Legal and Regulatory Uncertainties," Digital Transactions, July 24, 2013, http://www.digitaltransactions.net/interlink-starts-growing-again-and-visa-prospers-despite-legal-and-regulatory-uncertainties/.

[5] Douglas King, "Chip-and-PIN: Success and Challenges in Reducing Fraud," Retail Payments Risk Forum Working Group of the Federal Reserve Bank of Atlanta, January 2012, https://www.frbatlanta.org/-/media/documents/rprf/rprf_pubs/120111wp.pdf.

[6] "The WTO Agreements Series Technical Barriers to Trade," World Trade Organization, 2014, https://www.wto.org/english/res_e/publications_e/tbttotrade_e.pdf.

[7] "Global Standards: Building Blocks for the Future," U.S. Congress Office of Technology Assessment, https://www.princeton.edu/~ota/disk1/1992/9220/9220.PDF, 101.

[8] Masami Tanaka, "Tools for leaders – Demonstrating and exploiting the benefits of standards," *ISO Focus*+, June 2010, vol. 1 (6):1. https://www.iso.org/files/live/sites/isoorg/files/news/magazine/ISO%20Focus%2B%20(2010-2013)/en/2010/ISO%20Focus%2B%2C%20June%202010.pdf.

[9] Edwin Mansfield, Microeconomics Theory and Application (New York NY:W.W. Norton 1970)

[10] "A Guide to EMV Chip Technology Version 3.0," EMVCo, December 18, 2017, https://www.emvco.com/terms-of-use/?u=wp-content/uploads/documents/A-Guide-to-EMV-Chip-Technology-v3.0-1.pdf.

[11] ibid.

[12] Tim Büthe and Walter Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy*, (Princeton: Princeton University Press, 2011).

[13] "A Guide to EMV Chip Technology Version 3.0," EMVCo, December 18, 2017, https://www.emvco.com/terms-of-use/?u=wp-content/uploads/documents/A-Guide-to-EMV-Chip-Technology-v3.0-1.pdf.

[14] Carl F. Cargill, "Why Standardization Efforts Fail," *Standards* 14, no. 1 (2011), doi: http://dx.doi.org/10.3998/3336451.0014.103.

[15] "EMVCo Operating Principles," EMVCo, 2017, https://www.emvco.com/wp-content/uploads/2017/03/EMVCo-Website-Content-8.0-Operating-Principles-PDF_v1.1-1.pdf.

[16] Douglas King, "Chip-and-PIN: Success and Challenges in Reducing Fraud," Retail Payments Risk Forum Working Group of the Federal Reserve Bank of Atlanta, January 2012, https://www.frbatlanta.org/-/media/documents/rprf/rprf_pubs/120111wp.pdf.

[17] ibid.

[18] United States of America v. Visa U.S.A. Inc., Visa International Corp., and Mastercard International Incorporated, (98 Civ. 7076 BSJ) U.S. District Court Filed 10-9-2001 Southern District of New York

[19] Allie Johnson "U.S. credit cards becoming outdated, less usable abroad", CreditCards.com, October 1, 2008, https://www.creditcards.com/credit-card-news/outdated-smart-card-chip-pin-1273.php.

[20] Robin Sidel, "Debit-Card Use Overtakes Credit," The Wall Street Journal, May 1, 2009, https://www.wsj.com/articles/SB124104752340070801.

[21] "Debit Card Use Remains Robust in Midst of Economic Downturn," Pulse, June 14, 2010, last accessed July 11, 2019, https://www.pulsenetwork.com/news/archive/2010/debit-use.html .

[22] "Visa Recommended Practices for EMV Chip Implementation in the U.S.," Visa, July 11, 2012, https://technologypartner.visa.com/Download.aspx?id=153.

[23] "Visa Announces Plan to Accelerate Chip Migration and Adoption of Mobile Payments," Visa, August 8, 2011, https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.8916.html

[24] ibid.

[25] "Mobile Proximity Contactless Payment FAQ#1," EMVCo, July 2008, https://2426-9805.el-alt.com/best_practices.aspx?id=162.

[26] "Contactless Mobile Payment Architecture Overview," EMVCo, June 2010, https://www.emvco.com/wp-content/uploads/documents/Contactless_Mobile_Payment_Architecture_Overview_2010062808363068.pdf.

[27] "EMV Contactless Specifications for Payment Systems, Book A, Architecture and General Requirements Version 2.1," EMVCo, March 2011, https://www.emvco.com/wp-content/uploads/2017/05/Book_A_Architecture_and_General_Rqmts_v2_6_Final_20160422011856105.pdf.

[28] Fumiko Hayashi and Terri Bradford, "Mobile payments: Merchants' Perspectives," *Economic Review*, *Federal Reserve Bank of Kansas City*, Second Quarter (2014): 33-58, https://www.kansascityfed.org/~/media/files/publicat/econrev/econrevarchive/2014/2q14hayashi-bradford.pdf.

[29] "QR Code Specification for Payment Systems (EMV QRCPS) Consumer-Presented Mode, Version 1.0," EMVCo, July 2017, https://www.emvco.com/wp-content/uploads/documents/EMVCo-Consumer-Presented-QR-Specification-v1-1.pdf.

[30] "QR Code Specification for Payment Systems (EMV QRCPS), Merchant-Presented Mode Version 1.0," EMVCo, July 2017, https://www.emvco.com/wp-content/uploads/documents/EMVCo-Merchant-Presented-QR-Specification-v1-1.pdf.

[31] "Visa Best Practices for Data Field Encryption Version 1.0," Visa, October 5, 2009, https://bd.visa.com/dam/VCOM/global/support-legal/documents/bulletin-encryption-best-practices.pdf.

[32] "Visa Best Practices for Tokenization Version 1.0," Visa, July 14, 2010, https://usa.visa.com/dam/VCOM/global/support-legal/documents/bulletin-tokenization-best-practices.pdf.

[33] "Testimony of David Fortney The Clearing House Payments Company House Committee on Financial Services Subcommittee on Financial Institutions and Consumer Credit," Subcommittee on Financial Institutions and Consumer Credit, March 5, 2014, https://www.theclearinghouse.org/-/media/files/association-related-documents/20140305-david-fortney-testifies-on-tokenization.pdf.

[34] Jim Daly, "Interlink Starts Growing Again And Visa Prospers Despite Legal and Regulatory Uncertainties," Digital Transactions, July 24, 2013, http://www.digitaltransactions.net/interlink-starts-growing-again-and-visa-prospers-despite-legal-and-regulatory-uncertainties/.

[35] "Merchant community coalesces behind open process for security standards to better protect U.S. businesses and consumers from cybercriminal activity," PR Newswire, July 28, 2014, https://www.prnewswire.com/news-releases/merchant-community-coalesces-behind-open-process-for-security-standards-to-better-protect-us-consumers-and-businesses-from-cybercriminal-activity-268879481.html.

[36] "Mastercard, Visa and American Express Propose New Global Standard to Make Online and Mobile Shopping Simpler and Safer," Mastercard, October 1, 2013, https://newsroom.Mastercard.com/press-releases/Mastercard-visa-and-american-express-propose-new-global-standard-to-make-online-and-mobile-shopping-simpler-and-safer/.

[37] ibid.

[38] "EMV Payment Tokenisation Specification - Technical Framework v1.0," EMVCo, March 10, 2014, https://www.emvco.com/wp-content/uploads/documents/EMVCo_Payment_Tokenisation_Specification_Technical_Framework_v1.0.pdf.

[39] "The Fed Wants To Clean Up Token Confusion", Pymnts.com, September 29, 2014, https://www.pymnts.com/in-depth/2014/the-fed-wants-to-clean-up-token-confusion/

[40] "Visa CEO Predicts a 'Relatively Easy' Conversion to the New Secure Remote Commerce System", Digital Transactions, October 24, 2019, http://www.digitaltransactions.net/visa-ceo-predicts-a-relatively-easy-conversion-to-the-new-secure-remote-commerce-system/

[41] "EMV Secure Remote Commerce Technical Framework - Version 1.0," EMVCo, November 1, 2017, https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/Secure-Remote-Commerce-Framework-FINAL-v1.0.pdf.

[42] ibid.

[43] "EMVCo, FIDO Alliance, and W3C Form Interest Group to Enhance Security and Interoperability of Web Payments," W3C, April 17, 2019, https://www.w3.org/2019/04/pressrelease-wps.html.en.

[44] "EMVCO Secure Remote Commerce Specification, Version 0.9 DRAFT," EMVCo, October 19, 2018, https://www.emvco.com/wp-content/uploads/documents/EMVCo-Secure-Remote-Commerce-Specification-v0.9-2.zip.

[45] ibid.